



**NAVAL  
POSTGRADUATE  
SCHOOL**

**MONTEREY, CALIFORNIA**

**THESIS**

**AERIALLY DEPLOYED REAL-TIME TARGETING SENSOR  
NET**

by

Scott M. Diamond

June 2006

Thesis Advisor:  
Second Reader:

Orin Marvel  
Karl Pfeiffer

**Approved for public release; distribution is unlimited**

THIS PAGE INTENTIONALLY LEFT BLANK

## REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE June 2006	3. REPORT TYPE AND DATES COVERED Master's Thesis	
4. TITLE AND SUBTITLE Aerially Deployed Real-Time Targeting Sensor Net		5. FUNDING NUMBERS RIB57	
6. AUTHOR(S) Scott M. Diamond			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000		8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A		10. SPONSORING/MONITORING AGENCY REPORT NUMBER	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited	12b. DISTRIBUTION CODE		
13. ABSTRACT (maximum 200 words)  This thesis focuses on developing and analyzing a model for an aerially deployed real-time targeting sensor net to close the current gap that exists between the potential technological-doctrinal capability within society and that of the military. It outlines current real-time targeting need due to the decomposition of warfare after the fall of the Soviet Union, and portrays the targeting discrepancies in the Global War on Terror. From end-user surveys requirements are layed out for a system of systems to meet targeting needs. A feasible solution consisting of a system architecture anchored in existing commercial off the shelf technology is proposed to meet the discrete deliverables necessary to accomplish targeting goals to deal with asymmetric threats in opaque environments.			
14. SUBJECT TERMS Sensor Net, Targeting, Wireless Mesh, C2, Command And Control, Special Operations, Asymmetric Warfare, Capability Gaps, Technological Doctrinal Gap, Real Time Targeting, Systems Engineering, Reverse Engineering, Requirements Definition, Special Forces, Targeting, Decomposition, Real-Time, Ultra Wideband, TNT, COASTS, Aerial Deployment, Ad-Hoc Networks, Sensor Network, Sensor Feed, Common Operational Picture, EMF Detection, Complex Targeting, Real-Time Communication, Jungle Insurgency, ISR, Intelligence, Surveillance, Reconnaissance		15. NUMBER OF PAGES 115	
16. PRICE CODE			
17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT UL

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)  
Prescribed by ANSI Std. Z39-18

THIS PAGE INTENTIONALLY LEFT BLANK

**Approved for public release; distribution is unlimited**

**AERIALLY DEPLOYED REAL-TIME TARGETING SENSOR NET**

Scott M. Diamond  
Ensign, United States Navy  
B.S., United States Naval Academy, 2005

Submitted in partial fulfillment of the  
requirements for the degree of

**MASTER OF SCIENCE IN SYSTEMS TECHNOLOGY  
(COMMAND, CONTROL AND COMMUNICATIONS (C3))**

from the

**NAVAL POSTGRADUATE SCHOOL  
June 2006**

Author: Scott M. Diamond

Approved by: Orin E. Marvel, Ph.D.  
Thesis Advisor

Karl D. Pfeiffer, Ph.D., LtCol USAF  
Second Reader

Dan Boger, Ph.D.  
Chairman, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

## **ABSTRACT**

This thesis focuses on developing and analyzing a model for an aerially deployed real-time targeting sensor net to close the current gap that exists between the potential technological-doctrinal capability within society and that of the military. It outlines current real-time targeting need due to the decomposition of warfare after the fall of the Soviet Union, and portrays the targeting discrepancies in the Global War on Terror. From end-user surveys requirements are layed out for a system of systems to meet targeting needs. A feasible solution consisting of a system architecture anchored in existing commercial off the shelf technology is proposed to meet the discrete deliverables necessary to accomplish targeting goals to deal with asymmetric threats in opaque environments.

THIS PAGE INTENTIONALLY LEFT BLANK

## TABLE OF CONTENTS

I.	INTRODUCTION AND BACKGROUND DATA .....	1
A.	WARFARE DECOMPOSITION (UNBOUND WARFARE) .....	2
B.	VICTORY REDEFINED: SURVIVAL AND IDEOLOGY .....	5
C.	TECHNOLOGICAL DOCTRINAL GAP (TDG) .....	7
D.	PURPOSE OF THE STUDY .....	10
E.	RATIONALE .....	11
F.	THESIS OBJECTIVES AND RESEARCH QUESTIONS .....	12
G.	DEFINITION OF TERMS .....	14
H.	THESIS ORGANIZATION .....	15
II.	METHODOLOGY .....	17
A.	TOP DOWN APPROACH .....	17
B.	RESEARCH APPROACH .....	18
1.	Phase 1: Problem Definition .....	19
2.	Phase 2: Complex Targeting Research .....	19
3.	Phase 3: Concept (Model) Analysis .....	20
4.	Phase 4: Conclusions and Future Development ..	20
C.	COASTS FIELD EXPERIMENTATION .....	20
D.	END-USER DEFINED REQUIREMENTS .....	24
E.	ASSUMPTIONS AND LIMITATIONS .....	24
III.	TECHNOLOGY/LITERATURE REVIEW .....	27
A.	NEW FORM OF WARFARE .....	27
B.	TECHNOLOGIES AND IMPLICATIONS .....	28
1.	Sensor Nets .....	28
2.	Ultrawideband Sensors .....	29
3.	Information Dissemination .....	31
4.	Wireless Information Security .....	32
5.	Aerially Deployed Autonomous Sensor-Shooter Grid .....	33
6.	Wireless Mesh Communications Nodes .....	34
7.	Aerially Deployed Environmental Remote Sensors .....	35
8.	Remote Power Source Technology .....	35
9.	Miniaturized Sensor Webs .....	36
10.	Target Data Layered onto a Sensor Feed .....	37
11.	Networkable Aerial Sensors .....	38
12.	Static Aerial Sensor and Transmission Nodes ..	39
13.	Summary .....	40
C.	SENSOR REVIEW .....	40
1.	Ultra-Wideband Sensors .....	40
2.	Visual Feed Sensors .....	43
D.	CHAPTER SUMMARY .....	44

<b>IV.</b>	<b>MODEL ANALYSIS</b>	<b>45</b>
A.	NEED	45
1.	Need in Thailand	45
2.	Perceived Thai Problem	46
3.	COASTS Scenario Overview	47
4.	COASTS Scenario Overview	49
B.	REAL-TIME TARGETING PARADIGM PROBLEM	51
C.	SENSORS	51
1.	Small Shooter-Small Sensor	51
2.	Sensor Net Operations	56
D.	END-USER SURVEY	59
1.	Problem Definition	59
2.	Discrete Deliverables	59
3.	Ideal Equipment Requirements	60
4.	Ideal Doctrinal Requirements	62
E.	MEASURES OF EFFECTIVENESS ANALYSIS	63
F.	SYSTEM (MODEL) ARCHITECTURE	67
G.	AERIALLY DEPLOYED SENSOR NET	73
1.	Overview of the Model	73
H.	IMPLEMENTATION OF SENSOR NET	76
<b>V.</b>	<b>SYSTEM SOLUTION AND FUTURE DEVELOPMENT</b>	<b>79</b>
A.	FUTURE DEVELOPMENTS	79
1.	Path to a Solution	79
B.	FUTURE RESEARCH	82
<b>APPENDIX A.</b>	<b>ACRONYMS</b>	<b>85</b>
<b>APPENDIX B.</b>	<b>MEASURES OF EFFECTIVENESS</b>	<b>89</b>
<b>APPENDIX C.</b>	<b>COALITION OPERATING AREA SURVEILLANCE AND TARGETING SYSTEM (COASTS) THAILAND FIELD EXPERIMENT (MAY 2006)</b>	<b>91</b>
A.	BACKGROUND	91
<b>LIST OF REFERENCES</b>		<b>93</b>
<b>INITIAL DISTRIBUTION LIST</b>		<b>99</b>

## LIST OF FIGURES

Figure 1.	Illustration of the Technological-Doctrinal Gap..	7
Figure 2.	Special Operations Core Tasks.....	9
Figure 3.	Attempts to Fill the TDG for Sensor Technology in Homeland Security (From: Vent, 2005).....	10
Figure 4.	Top-Down Development Process.....	18
Figure 5.	COASTS 2006 Network Topology.....	23
Figure 6.	COASTS 2006 Communications Network Model.....	24
Figure 7.	SOSUS Acoustic Sensor Network.....	29
Figure 8.	Ultra Wideband (UWB) Video Sensor Looking through Wall(From: Herzig, 2005).....	30
Figure 9.	UWB Video Link (From: Herzig, 2005).....	30
Figure 10.	UWB Sensors Looking through a Wall (From: Herzig).....	31
Figure 11.	UWB Sensor Generating a Video Stream from Reflected Wavelengths through a Wall (From: Herzig).....	31
Figure 12.	Illustration of Link-16 Interoperability.....	32
Figure 13.	SecNet 11 NSA Approved Encryption.....	33
Figure 14.	CBU-97 Sensor Fuzed Weapon.....	34
Figure 15.	Mesh Dynamics Wireless Mesh Box.....	35
Figure 16.	Gridpoint Remotely Managed Renewable Power Source.....	36
Figure 17.	Webbed Pods Created by NASA and NOAA in "The Link Project".....	37
Figure 18.	Gumball Size Wireless Sensor Pod.....	37
Figure 19.	Large Sized CyberBug Launch.....	38
Figure 20.	Networked VTOL Mobile Aerial Sensor.....	39
Figure 21.	Visual Sensor and Information Node.....	40
Figure 22.	Signal Comparison against Noise Threshold.....	41
Figure 23.	Full Duplex Handheld UWB Transceiver.....	42
Figure 24.	UWB Precision Geolocation System Transceiver....	42
Figure 25.	Event Breakdown for the Mae Gnat Dam Drug Interdiction Scenario.....	50
Figure 26.	Current Recognized Principles of War.....	53
Figure 27.	The Real-Time Sensor Cycle.....	54
Figure 28.	Special Operations Liaison Element Functions (From: JSOTF Pub).....	55
Figure 29.	Common Operational Picture Displaying UAV Sensor Feed FOVs, TDD, and Friendly Overlay....	56
Figure 30.	Aerial Sensor Feed Overlayed with TDD, Friendly Data, and Sensor Feed Priority.....	57
Figure 31.	CyberDefense CyberBug Gimbaled Visual Sensor Feed.....	59

Figure 32.	RQ-11 Raven Squad Level UAV.....	61
Figure 33.	RQ-1 Predator UAV.....	62
Figure 34.	Sensor in Depth Layers.....	74
Figure 35.	RQ-4 Globalhawk ISR UAV Similar to the U-2 Spy Plane.....	75
Figure 36.	Ruggedized MTM Micro Tablet by Modular PC (From: <a href="http://modular-pc.com/">http://modular-pc.com/</a> , Retrieved March 2, 2006) .....	80

## **ACKNOWLEDGMENTS**

I would like to thank Professor Marvel for his brilliant insight and methodology. His class inspired me from the beginning.

I would also like to thank COL Pfeiffer for vectoring me onto target and the COASTS team for an incredible opportunity and their support.

Thank you to SPAWAR SSC for the funding and their belief in my ideas, and to the COASTS research group for the opportunities and experiences.

And most of all my Mom and Dad, who supported me throughout this endeavor.

THIS PAGE INTENTIONALLY LEFT BLANK

## I. INTRODUCTION AND BACKGROUND DATA

Today's ever-changing military environment is best described by Jackowski (2002). He explains that military missions "are being redefined daily due to rapidly changing world situations and the call for fighting in different types of conflict...New emerging technologies that are revolutionary will be deployed [in the near future] that will really change current military operations" (p. 2).

The literature has acknowledged the fact that technologies are continuing to change and evolve, even at the present time (Aloul & Aboelaze, 2005; Nekoogar, 2005; Suh & Horton, 2004). Internet Protocol version 6 (IPv6), Voice over Internet Protocol (VoIP), and high speed networks, for example, are now everyday capabilities and expectations. The Internet is also growing with respect to its dimensions - networks are evolving from land-based facilities to composite network based entities, now called net-centric networks (Bowie, Haffa, & Mullins, 2003; Jackowski, 2002). These are comprised of land, air and space modules. In the view of Jackowski (2002), The Net-centric network:

...promises to be the most revolutionary improvement in network-enabled operations by rapidly getting critical information to the right individual or organization, thereby significantly improving the efficiency and speed of combat operations. In essence, the major areas influencing military operations are new government directed missions driven by world events and rapidly changing enabling technologies... (p. 2).

Clearly, change is constantly taking place at an accelerated rate with regard to military operations to keep up with the times and the new technology. As Jackowski (2002) has noted, "all the new technologies must be fully integrated into a comprehensive military architecture as early as possible" (p. 2) because warfare has changed as well. In order to understand the purpose and objectives of the present thesis, it is first necessary to provide an overview of warfare changes in terms of decomposition, a redefinition of victory in terms of survival and ideology, and the current technological-doctrinal gap that currently exists.

#### **A. WARFARE DECOMPOSITION (UNBOUND WARFARE)**

After the Cold War world dissolved the Soviet Union in the 1990s many expected tranquility to follow. However, the weapons of war remained, and just because the Command and Control structure had dissolved from the top down, the basic elements did not disappear. Instead they consolidated after decomposing into their component parts. In Yugoslavia, the decomposition was called ethnic nationalism. In Rwanda, it was called tribalism. Like droplets of water coagulating around dust particles, forces were rebound around their arms. Why? Because they had the option of violence and a new found self-organization to achieve their objectives. They had been born into a culture of violence, the fear was not there, they had been desensitized to the violence. These decompositions took place in formerly controlled locations of Soviet rule, such

as Somalia and Afghanistan. "The world now faces a particularly virulent array of decomposed forces, bound through ideology" (Braden, 2006, p. 61).

This force decomposition requires an interoperable modularization of our forces. This means that the greater forces must be broken down into component parts which can be tailored to the basic sensing-output delivery missions. Such sensor missions vary from location to location. In environments consisting of dense foliage, for example, sensors can be hung in the trees, whereas aerial coverage is not feasible. Conversely, desert (which is the current operating environment for the majority of US operations) does not lend itself to ground sensors; aerial sensor operations are optimal. The entire mission package must be tailored to the operation, location, and enemy. This is the essence of a modularly delivered force that is required of this new form of unbound, decomposed warfare (Bowie, Haffa, & Mullins, 2003).

Warfare today is intrinsically a joint operation because of the decomposition of opposing forces. However, the disadvantage of joint operations is that it combines two large ungainly forces into one - multiple bureaucracies and/or multiple chains of command (Joint Vision 2020, GPO 2000). As seen in the recent special operations intensive conflicts of Operation Enduring Freedom and Operation Iraqi Freedom jointness often leads to communication and coordination issues that can intensify the fog of war and ultimate cost lives. Documents such as Joint Vision 2020 (GPO, 2000) and Sea Power 21 (Clark, 2002) which shape U.S. national military strategy call for the use of unattended sensor networks to provide persistent intelligence,

surveillance, and reconnaissance (ISR). The evolution of integrated circuits, wireless communications, and data networking makes unattended, wireless sensor networks practical for military and law enforcement applications (Bach & Fickel, 2004; Chong & Kumar, 2003; Karlof & Wagner, 2003; Halvardsson & Lindberg, 2004).

Sensor and shooter are rarely the same platform today. The concept of distributed Command and Control (C2) is being implemented downwards to the tactical level. Platforms are reaching absolute levels of sensor/shooter automation while the boundaries between force effectiveness' are blurring as combined arms and joint doctrines employ systems of systems. Technological capability continues to accelerate past the doctrinal/conceptual boundaries of today's military, and the Global War on Terror (GWOT) has opened up new fronts around the globe and shifted the threat of war from nationalistic targets to ideological targets. There is no clear front anymore. The front is global, and the tactics are asymmetric.

Refinement of distributed targeting is a necessity in order to combat current and future threats in the GWOT with Joint Forces. Complex Targeting in a desert environment has proven feasible in OIF where visibility is not limited by flora. However as operations continue to expand around the globe in the GWOT, American forces will face the challenge of diverse opaque environments (OE) where extremist ideologies hostile to the United States and American interests also reside.

The GWOT is essentially a war without boundaries or fronts (Shreves, 2004). Forces and weaponry have

decomposed into component parts comprised of individual persons with personal communications capabilities for a direct mesh of information flow between the edges.

#### **B. VICTORY REDEFINED: SURVIVAL AND IDEOLOGY**

Today the country does not face a national threat as before. The previously understood threat has decomposed doctrinally and geographically and continues to progress into the next phase of warfare (Shreves, 2004). Just as many look back upon military tactics of the civil war as obsolete, so too will the current capability of warfare be viewed in the one day in the future.

Group survival today relies upon a group ideological replication, not the traditional notion of genealogical survival. Small nations such as Singapore exist and produce great capital with very few national resources. Land is no longer a necessary goal of conquering nation states. Conquering the world's information real estate is. It is the next level of Darwinian survival. During times of tribal life man sought the survival of his individual genes. Once humans began to organize into larger groups they fought for group physical survival. To survive and replicate genes in this type of society required land and resources.

In the first world, today's sense of survival has become rooted in the propagation of ideology. As Shreves (2004) has pointed out, "Much has been written recently on how terrorism is a tactic and not an enemy" (p. 3) thus supporting the view that survival is indeed related to ideology. Historically, ideas have emerged and demanded their own survival - Christianity, Islamic fundamentalism,

etc. - these sought to replicate across human minds by their intrinsic nature. Today we have reached a societal apex satisfying physical needs, and moved onward to ideological survival and competition of mutually exclusive ideologies. It is this self replication of mental real estate which is the source of today's conflicts, and in an information age, the replication of ideas is rapid and competitive. Historically, ideological replication depended on roadways and physical lines of communication. Today information flows freely even through the borders of the most repressive regime, and the freedom of information is one of the fundamental elements that appears to have catalyzed the decomposition of warfare and redefined victory.

It is this global flow of ideologies that influences everything from the strategic to the tactical level and requires a rewrite of doctrine. Attrition warfare was created to fight in the plane of physical survival. Guerilla warfare was created to make war on the local ideological plane. A new plane of global information warfare must be created to combat the ideological threat being faced in today's society.

Contrastingly, this warfare is simplified because of it's decomposition of forces; however this requires a greater modularity because of variability of battlespaces. Physical survival used to be regionally bound by resources and countries. The rules have changed for ideological survival. Individuals now have access to national level ideas that formerly required large organizational support to propagate. The individual is now empowered with the ability from the tactical level to flow information up to a

global audience and achieve strategic goals. This person can now utilize commercial off the shelf (COTS) technology to achieve strategic goals, while at the same time, utilizing that technology to downlink strategic ideological goals and operate independent of national tasking, and carrying out the basic principles of exclusive ideological replication.

### C. TECHNOLOGICAL DOCTRINAL GAP (TDG)

Technology has moved beyond traditional doctrinal and conceptual understanding within the collective military mind (Figure 1).

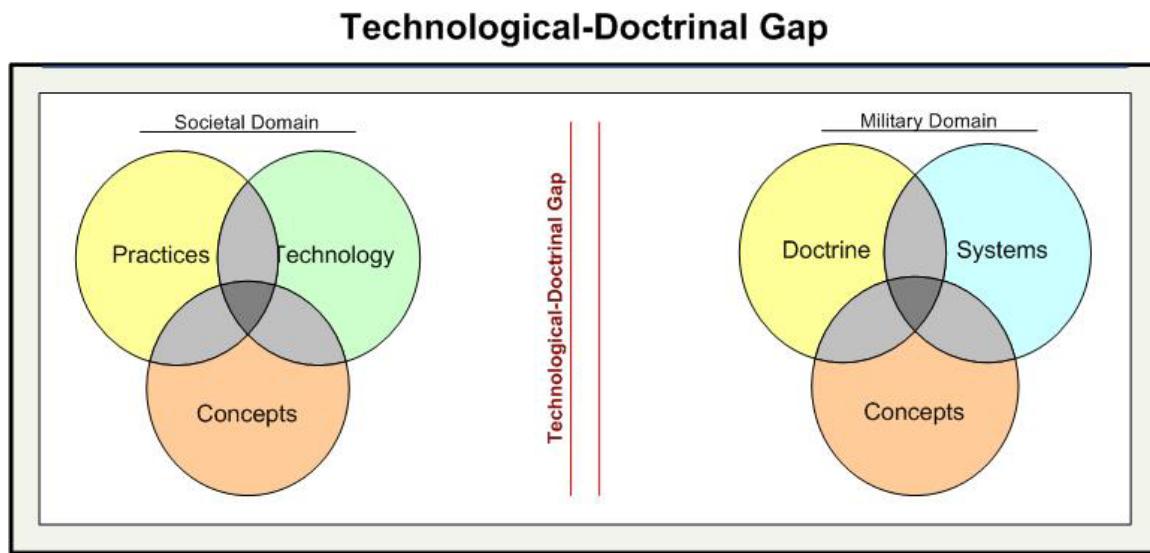


Figure 1. Illustration of the Technological-Doctrinal Gap

Military doctrine today is based on tried and true methods that have been proven, are acceptable, clearly work and are cost-effective. People with corporate knowledge get the job done. For the majority of the military, explicit and tacit doctrine favors antiquated methodologies and technologies.

As a result, there are technological capabilities not exploited by our military. Specifically, there is a technological-doctrinal gap between potential sensor capabilities based upon society's technological level and current conceptual understanding/doctrinal practices (Akyildiz, Weilian, Sankarasubramaniam, & Cayirci, 2002; Caimu & Raghavendra, 2005; Fraden, 2004). Given the input of a location in either absolute or relative coordinates the desired change of state - whether it be weapons action or otherwise - can be produced in real-time (given assets are within range).

That reactionary capability has now been achieved. The failure is producing the location output given raw emissions from a target. We depend upon too primitive detection methods of raw emissions from enemy units. If a target is emitting or reflecting detectable emissions that raw data should be converted into a location output that can effectively be used to produce a targeting solution for weapons action in real-time. It is important to note that there are EMF emissions (subcategorized into reflected and emitted) and acoustic emissions, mostly emitted (Aboelaze & Aloul, 2005).

Given the lack of bounding of enemy forces that must be detected - now ideologically bound and highly variable - this capability must be highly modularized and made to be interoperable. In studies and general experiences with the military detected what is loosely labeled as the technological-doctrinal gap (TDG). This gap, especially related to wireless sensor networks (see Pahlavan & Krishnamurthy, 2004) is a model for the discrepancy that exists. Figure 2 lists core tasks of special operations.

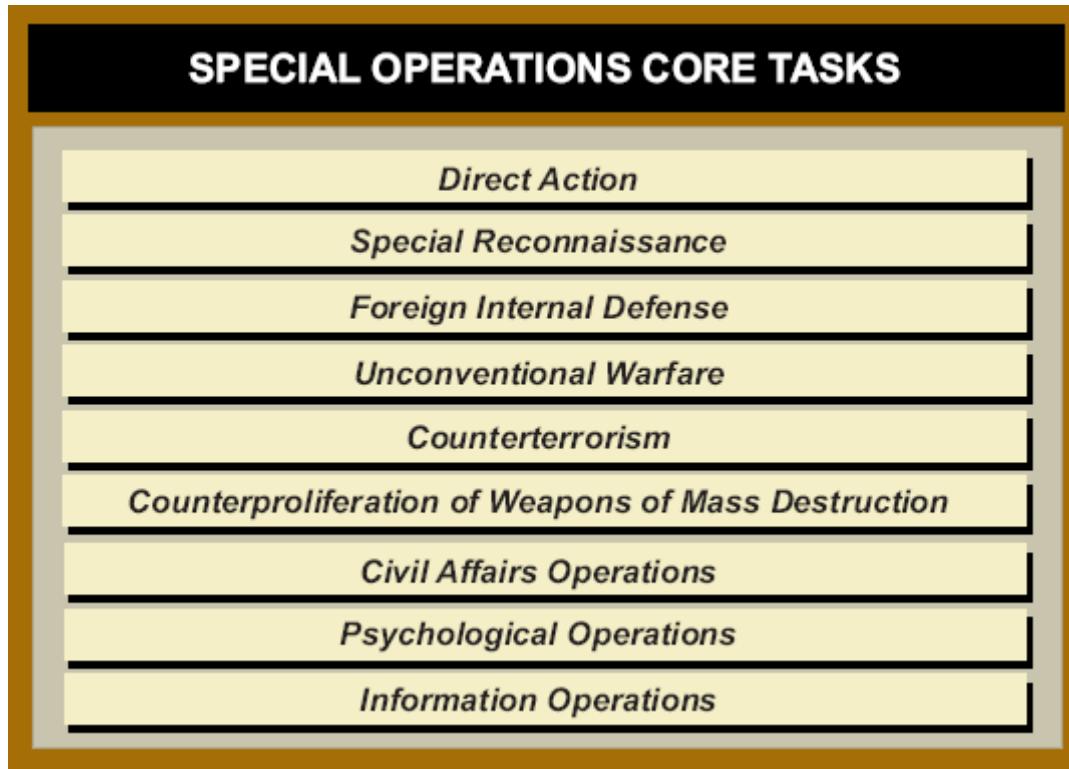


Figure 2. Special Operations Core Tasks

Notice the lack of a targeting paradigm or description. Instead, targeting is an implied element in each of these tasks but not the focus. Targeting doctrine should be developed as a task to supplement each of these tasks. These highlight the TDG in the sense that there is a lack of a doctrinal paradigm for focusing real-time targeting operations to streamline and bootstrap existing tasks.

The presence of the TDG is concluded from the correlation of several technological and doctrinal items seen in both civilian and military sectors of our society. These are highlighted in Figure 3 which shows an attempt to fill the TDG for sensor technology in homeland security.

## The Challenge Defined – an example

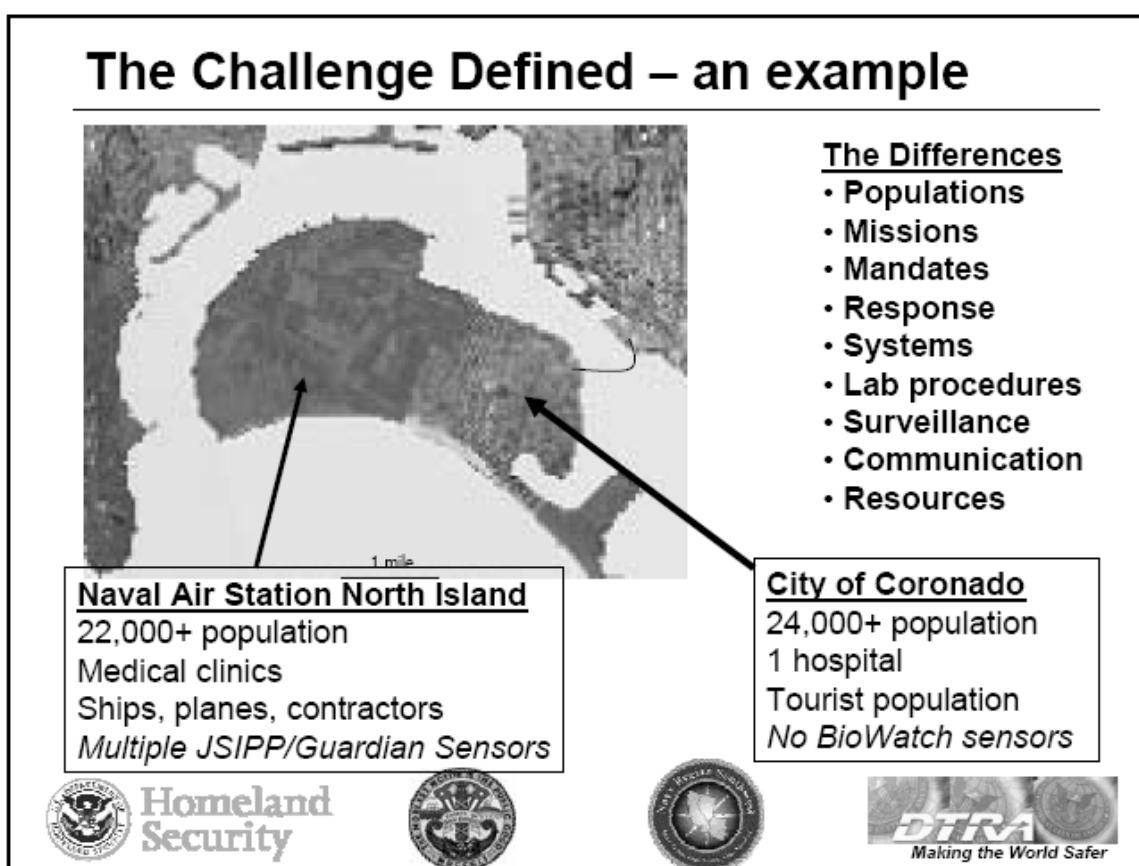


Figure 3. Attempts to Fill the TDG for Sensor Technology in Homeland Security (From: Vent, 2005)

### D. PURPOSE OF THE STUDY

The purpose of this thesis is to evaluate a model – that is, a system of systems. This model will be based on fundamental concepts to define targeting problems and provide support and background for a potential solution to sensor deficiencies. The model will help us determine how to overcome these deficiencies through an aerially deployed wireless mesh sensor network which acquires targeting data through a net of sensors utilizing a surrounding wireless cloud as the information medium to pass multi-layered target data and sensor feeds through interoperable gateways (high frequency (HF), very high frequency (VHF), ultra high frequency (UHF), Link-16, or otherwise) to the shooter(s).

Thus, this thesis focuses on a system of systems - top level technologies, doctrines, and tactical concepts required for the development of special operations forces (SOF)/air power mission accomplishment. This system of systems purports to use the Coalition Operating Area Surveillance and Targeting System (COASTS) research program (see Appendix C) at the Naval Postgraduate School (NPS) as a tropical-location test bed for equipment and ideas.

#### **E. RATIONALE**

This thesis was founded on the vision that there is a solution to be found to the problems and requirements for the GWOT and the rapidly changing nature of warfare within the current technological capacity of our society. The vision is to solve the issues of this new form of ill-defined warfare using current techniques, technology, and doctrinal capabilities. Some label the new form of asymmetric warfare faced today as unconventional, special, or military operations other than war (MOOTW); however, it is proposed to fundamentally be decomposed into the empirical elements of warfare. This decomposition was catalyzed by the fall of the Soviet Union, which provided enhanced capabilities to the decomposed elements which in turn were allowed to restructure and reorganize at a grass roots level.

It is this new threat of these decomposed elements that this thesis seeks to address. Through the leveraging of untapped societal technological capabilities and the empirical units of warfare cycles in real-time the US

forces can effectively leverage prosecution capabilities against the enemy as is demanded by the strategic objectives of the United States.

To highlight the ideas embodied in this work, an analysis of the current GWOT operations needs to take place in terms of desert environment versus triple canopy targeting. In Iraq the environment is essentially transparent to visual, infrared (IR), and near IR wavelength classes of sensors. However, in OE situations where targets cannot be sensed by direct reflections or emissions, issues arise with targeting operations. Urban operations are declared bloody casualty rich operations because of the opaque nature of the urban environment which allows decomposed enemy units to ensnare the military within their lower capability level of the sensor-shooter cycle highlighting US military sensor deficiencies.

In the opaque environment (OE) of Vietnam this was consistently the case. American forces retained weapon superiority throughout the war, but relied on the basic visual or acoustic contacts of foot patrols to output targeting data to shooters and prosecute the target. Often, sensor and shooter became the same unit, placing human life on the line as the sensors to gather targeting data. Today in the global environment produced by free information flow, this life losing deficiency in sensor capability is not acceptable.

#### **F. THESIS OBJECTIVES AND RESEARCH QUESTIONS**

The objective of this investigative thesis is to provide a proposed model, or system of systems based upon currently feasible technologies and the conceptual

doctrines/capabilities to augment the solution. To combat this new form of decomposed warfare a flexible and modular targeting system need be employed to detect the empirical units of war and produce outputs that can be utilized to leverage superior weapons capabilities.

In proposing a paradigm to further enhance strategic development of warfare for the United States, this proposed system will incorporate a system for rapid deployment. This insinuates an aerial delivery system not unlike that of the sonobuoy acoustic sensor system or the CBU-97/CBU-105 Sensor Fuzed Weapon (SFW). In addition, to cover the wide areas in OE's the sensor net will need to autonomously share and fuse multiple data feeds into a coherent real-time common operational picture (COP) to complete two tasks: (1) provide the knowledge necessary for situational awareness (SA) and target discrimination and (2) output the data for target prosecution by the shooter(s).

In summary, this thesis is an independently tasked contribution to the strategic objectives of the United States of America. Its supreme objective is to contribute to the next paradigm of warfare principles and meaningful progress towards the strategic objectives of the United States.

Based on the objectives stated above, the following research questions have been identified:

1. What are the underlying causes of current targeting problems?
2. What are the empirical causes of these problems?
3. What is a model for a solution to these problems?
4. Can a solution be feasibly accomplished with currently available technological-doctrinal capabilities?

## **G. DEFINITION OF TERMS**

Several common terms listed below are uniquely used in the study:

1. *Battlespace*: Dawidowicz (2001) defines this term as "the topology of the physical space where the action is taking place, the physical laws, the involved equipment and the entities' physical attributes" (p. 1).

2. *Net-Centric*: This designation refers to any entity or service that centers around the Internet and involves some type of computing system. A net-centric approach refers to the method used by a community of interest (agency, group, division, unit, etc.) brought together through a social network that aligns itself with Internet and computerized metadata. According to Zenishek and Usechak (2002), "a net-centric enterprise [whatever the form] must be implemented using open standards, non-proprietary APIs, loose coupling between data and applications, and agile (i.e., not fragile) interfaces" (p. 218).

3. *Measures of Effectiveness and Performance*: Measures of effectiveness (MOE) refers to a qualitative description of the desired parameters of the system (e.g. "the system will identify if the target is carrying a weapon"). A listing of these can be found in Appendix A at the end of the thesis. Measures of Performance (MOP) refer to a quantitative definition of the desired capabilities of the system (e.g. range, spectrum, etc.).

4. *Small Sensor - Small Shooter*: It is best to have a small sensor footprint. Today's global situation demands surgically striking without getting shot. Striving to achieve this is an ideal, but not often realistic.

5. *Real-Time Targeting*: Rather this thesis focuses on the current realized need for the accurate, high-tempo, and real-time targeting of high value targets. However, the fundamentals proposed can be rescaled to analyze larger targeting missions.

6. *Technological-Doctrinal Gap*: This refers to a lack of doctrinal understanding for focusing real-time targeting operations to streamline and bootstrap existing tasking.

#### **H. THESIS ORGANIZATION**

Chapter I introduces the study. It explains the topic, background of the problem, and the purpose of the study. It also redefines the meaning of victory and describes warfare decomposition. In addition, it provides research questions and definitions of terms that are unique to the study.

Chapter II details the methodology of the research study. Included is an explanation of the thesis structure, approach and method, assumptions, and limitations.

Chapter III reviews the pertinent technology literature. It details technology reports, sensor studies, fundamentals of warfare and network centric warfare.

Chapter IV provides a suggested model for real-time targeting - that is, a system of systems through an aerially deployed wireless mesh sensor network conceptualized from support in professional literature and research experiences.

Chapter V concludes the study. It brings together the separate modular components into a unified whole. It suggests a system solution and provides a path relevant to future developments.

## **II. METHODOLOGY**

### **A. TOP DOWN APPROACH**

This thesis was written with a top down approach as shown in Figure 4. Need and problems are defined first followed by paradigm development, refinement, and solutions. First and foremost, need is identified. Second, requirements are defined through an end-user perspective derived from operators and refined into measures of effectiveness and performance.

It is important to note that this thesis and the resulting model were developed through an evolutionary process. Techniques were developed, evaluated, and accepted or discarded based upon anticipated effectiveness. The methodology evolved with the writing of the thesis to optimally transfer information to the reader taking full advantage of the benefits of transferring information visually through figures and diagrams.

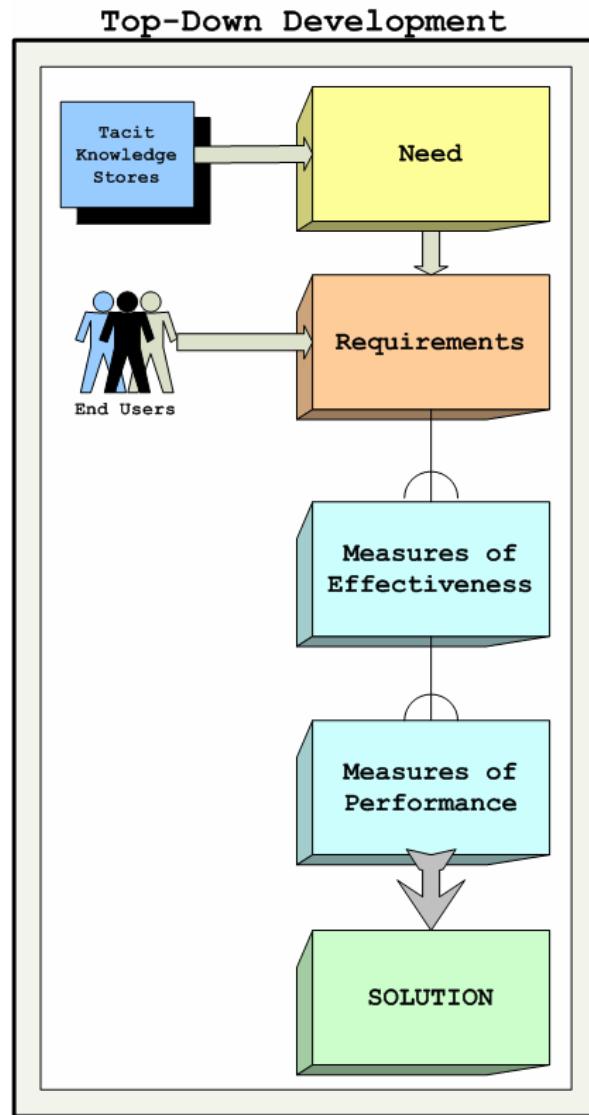


Figure 4. Top-Down Development Process

#### **B. RESEARCH APPROACH**

The present study represents qualitative research in that information is collected from researcher experiences, findings from the literature review, and conclusions were made from supporting experiences. In qualitative research, according to Creswell (2003), the researcher must ensure that the data collected is an accurate representation of the subject being studied, is comparable with known information, and is verifiable across subjects and

situations. This is necessary with qualitative research because this type of investigation emphasizes the uniqueness of human situations and experiences that are not necessarily accessible to validation through traditional (quantitative) forms of empirical evidence (Creswell, 2003). In light of this restriction, the quantitative terms reliability and validity are replaced with more qualitative terms, dependability and credibility. The research approach and method of the study draws on past and current studies, reports, and related material in addition to researcher experience. Experience data was supported by findings from authoritative studies, when possible.

The methodology of the present investigative research focused on developing concepts leading to the suggestion of a model - that is, a system of systems. Thus, the research method was divided into phases. These are described as follows.

### **1. Phase 1: Problem Definition**

Phase 1 involves the provision of basic definitions of current global requirements for complex targeting based upon geo-political climate/geographical concerns. Current problem of complex targeting must first be defined and a thorough statement of need developed. From the problem definition and the statement of need requirements are developed.

### **2. Phase 2: Complex Targeting Research**

This phase involves research of current techniques, technologies, and doctrine for complex targeting. This phase includes the necessary academic review of existing technical material, techniques, and doctrine utilized in complex targeting in both triple canopy rainforest and

other environments. The academic review will include verbal interviews of end-users. The review will take an end-user, top down view to development a comprehensive needs statement. Shortfalls in the linkage of doctrine to technology will be discussed and examined.

### **3. Phase 3: Concept (Model) Analysis**

Once thorough research of current technologies, doctrine, training, and current operations/cases has been completed, an encompassing conceptual model is developed - one that employs appropriate technologies, training, and personnel to accomplish the well defined complex targeting mission. During the development of the concept MOE's will be created to objectively evaluate future results.

### **4. Phase 4: Conclusions and Future Development**

The final phase consists of analyzing the system requirements and MOE's to develop a proposed system architecture and a legitimate path for future systems development

## **C. COASTS FIELD EXPERIMENTATION**

The concept underlying the COASTS program emulates a very successful ongoing NPS-driven field experimentation program entitled the NPS-U.S Special Operations Command Field Experimentation Program (NPSSOCFEP) (see Appendix C). This program has been active and successful since 2002 (*COASTS Thailand Field Experiment*, 2006). Right from the start this program supported USSOCOM requirements for integrating emerging wireless local area network technologies with surveillance and targeting hardware/software systems. The purpose was to augment SOF missions.

Since its inception, NPSSOCFEP has significantly grown. Today it includes almost a dozen private sector companies, several Department of Defense (DOD) organizations, and various academic institutions that contribute resources. An important activity of NPSSOCFEP is to conduct quarterly complex experiments to:

- Provide an opportunity for NPS students/faculty to experiment/evaluate the latest technologies which have potential near-term application to the warfighter.
- Provide operational experience to students/faculty.
- Provide military, national laboratories, contractors, and universities an opportunity to test and evaluate new technologies in operational environments; and implement self-forming multi-path, ad-hoc network w/sensor cell, ground, air, and satellite communications (SATCOM) network components.

COASTS 2005 used wireless local area network technologies to bring together data from ground and air sensors to a real-time, tactical C2 center. The successful display of capability clearly indicated United States Pacific Command dedication to encourage technology development and coalition warfare. Results of the experiment were shared with such countries as South Korea, Singapore, Thailand, Australia, and South Korea (*COASTS Thailand Field Experiment*, 2006).

COASTS 2006 will expand on the previous experiment and integrate the technology capability into a larger system of systems in support of tactical action scenarios in the form of an air, ground, and water-based scenario north of Chiang Mai, Thailand. Collection of tactical information will be displayed and distributed in real-time centers. This fusion

of information will authenticate the use of wireless communication mediums and test and evaluate the 'last mile' solution for the disadvantaged user.

It is important to explain that COASTS is a small unit network-capable communication and threat warning system that uses an open, plug-and-play architecture. This type of structure can be customized - that is, configured by the user.

Building self-configurable systems is most desirable, according to Subramanian and Katz (2000). It is possible to employ wireless ad-hoc networks, SA software applications, air balloons, UAVs, and biometrics capabilities, among other capabilities. All included components communicate through wireless network technology.

COASTS 2006 provides a testing and experimental setting for both Thailand as well as the United States. In this setting operational testing, field validation of newer wireless technologies, and integration can take place.

A number of research elements were addressed during the 2006 experiment. These include 802.11 b Distributed Sequence Spread Spectrum (DSSS); 802.11a/g Orthogonal Frequency Division Multiplexing (OFDM); 802.16 OFDM (Stationary); 802.16 OFDM (Mobile); SATCOM; and SA Overlay Software. In addition, wearable computing devices were tested as well as mobile C2 platforms. Shown in Figures 5 and 6 are the COASTS 2006 network topology and communications network model.

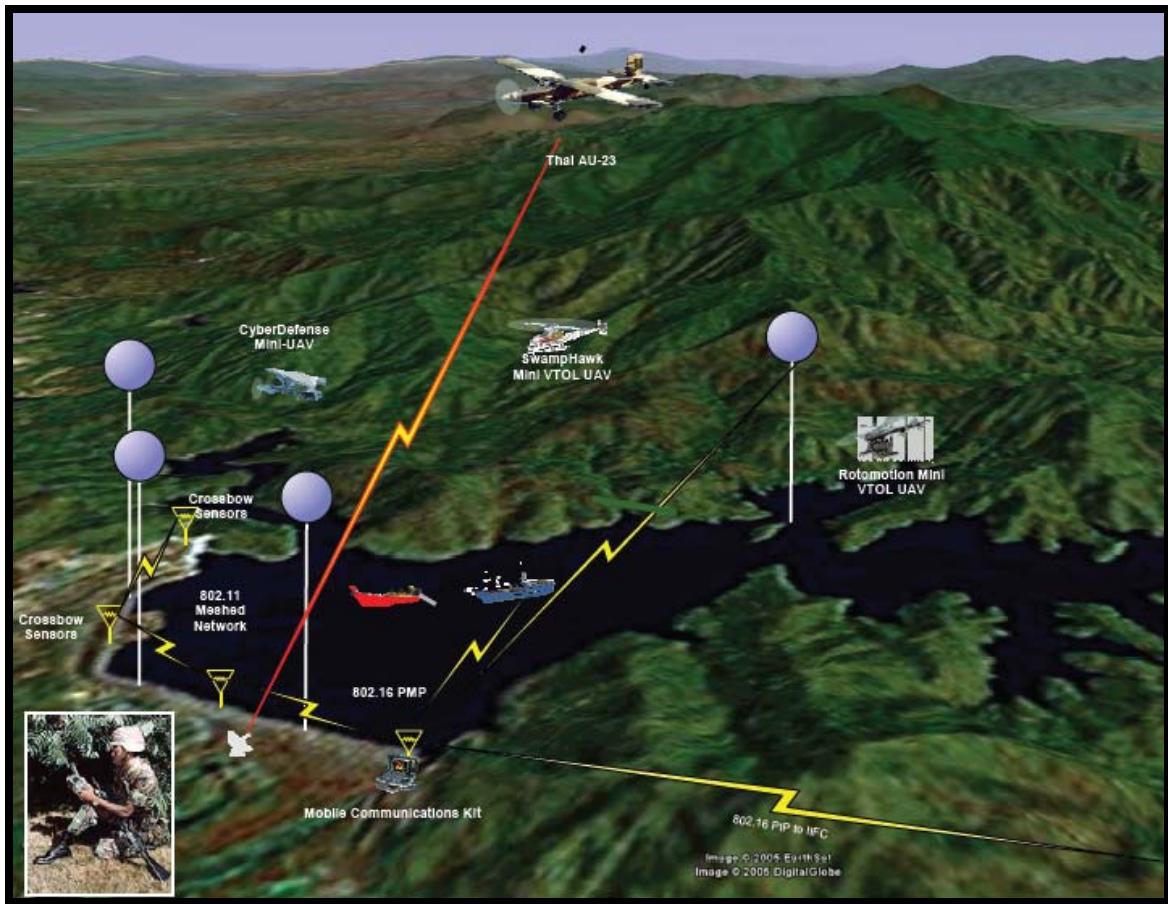


Figure 5. COASTS 2006 Network Topology

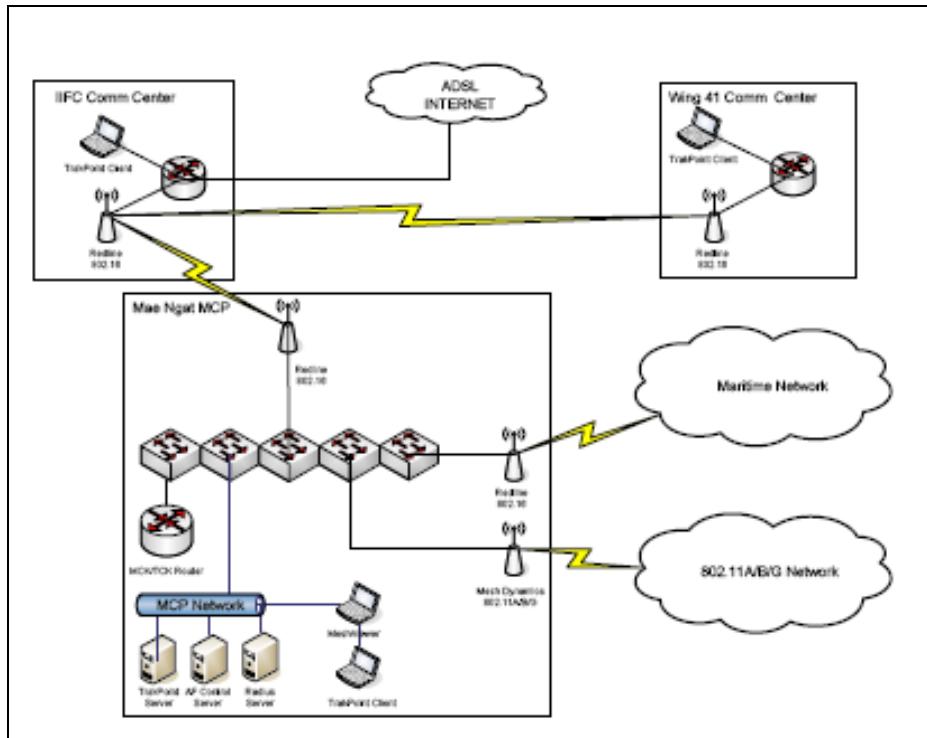


Figure 6. COASTS 2006 Communications Network Model

#### D. END-USER DEFINED REQUIREMENTS

Qualitative requirements were derived from End-User Interview of Special Forces Personnel with experience operating in the Philippines Area of Operations. This area of operations (AO) includes the Triple Canopy OE Jungle and Urban Centers where insurgents intermix with non-combatants.

#### E. ASSUMPTIONS AND LIMITATIONS

Below is a list of assumptions and limitations used for this thesis:

1. There exists a technological doctrinal gap (TDG).
2. There is a current need for a more proficient targeting system.
3. Combat will mostly be performed below the divisional level in the future.

4. Sensors are a detectable vulnerability.
5. With regard to sensor discrepancy, there are currently a number of issues associated with producing outputs from full spectrum emissions.
6. This thesis was restricted with regard to scope in terms of finances and time.
7. It is assumed that there can be a scalable solution with respect to affordable real-time targeting through an aerially deployed wireless mesh sensor network.

THIS PAGE INTENTIONALLY LEFT BLANK

### **III. TECHNOLOGY/LITERATURE REVIEW**

The previous portion of this thesis introduced the subject of concern, provided background information, stated the purpose, and presented the objectives and research questions. The purpose of this chapter is to review the technology literature relevant to the major focus on the study. The new form of warfare is examined first. The subject of technologies and implications is reviewed next, followed by a section on sensors.

#### **A. NEW FORM OF WARFARE**

The Counter Insurgency (COIN) Academy in Baghdad has been specifically established to address the needs of the emerging requirement of victory in the new form of warfare (Ricks, 2006). Being compulsory for all officers to take, it requires:

The School's textbook, a huge binder, [which] offers the example of a mission that busts into a house and captures someone who mortared a U.S. base.

On the surface, a raid that captures a known insurgent or terrorist may seem like a sure victory for the coalition,' it observes in red block letters. It continues, 'The potential second- and third-order effects, however, can turn it into a long-term defeat if our actions humiliate the family, needlessly destroy property, or alienate the local population from our goals (Ricks, 2006, p. A10).

The handbook attempts to address the essential underlying cause of tactical victories turning into strategic losses. Information propagation in itself is not

inherently a detriment to U.S. forces. The fidelity of the information being spread and the bias lent to that information are what cause strategic steps backward.

It is also important to understand that fragments of information can cause more damage than an individual Improvised Explosive Device (IED) to strategic objectives. Data fragments can spread, support, and plant the seed for the ideology of hate that tasks the people to conduct such operations of terrorism against the Western World. Consequently, it is this ideology that must be combated with precision operations.

This emerging requirement for victory requires a high level of precision, but not just precise weapons action (that capability has already been acquired), but precise target detection.

## **B. TECHNOLOGIES AND IMPLICATIONS**

The following review focuses on technologies and their respective implications. For the sake of brevity, various technologies of importance are cited in terms of items below, followed by conclusions.

### **1. Sensor Nets**

The technology exist and was developed when the need was catalyzed by Cold War operations in the past Sonobuoys and the Sound Surveillance System (SOSUS) system were developed from the threat of nuclear destruction during the Cold War (Figure 7).

- **Conclusion:** Acoustic sensor technology exists.
- **Conclusion:** A form of rapidly deployable sensor net technology exists
- **Conclusion:** Real-time targeting network technology and doctrine exists.

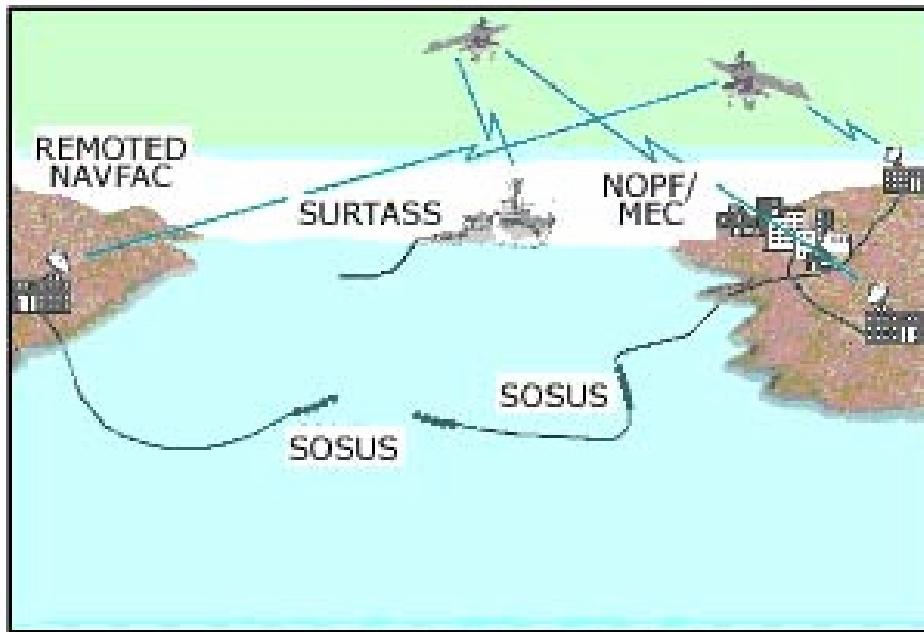


Figure 7. SOSUS Acoustic Sensor Network

## 2. Ultrawideband Sensors

The technology exists to actively output, sense, analyze, and display reflected wideband electromagnetic energy. The raw data can be processed to classify a target (Figure 8, 9, 10, and 11).

- **Conclusion:** The technology for highly sensitive and flexible sensors with the ability to autonomously produce discriminating data exists.
- **Conclusion:** The capability for real-time sensor feeds layered with target data exists.



Figure 8. Ultra Wideband (UWB) Video Sensor Looking through Wall (From: Herzig, 2005)

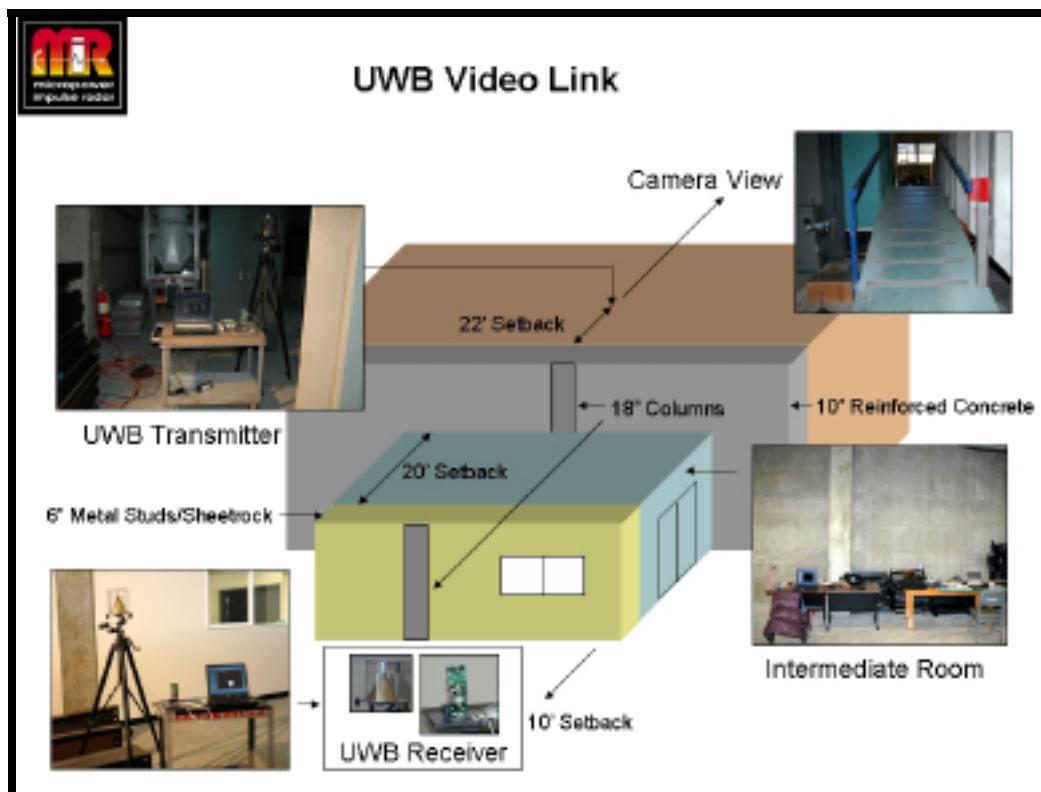


Figure 9. UWB Video Link (From: Herzig, 2005)



Figure 10. UWB Sensors Looking through a Wall (From: Herzig)



Figure 11. UWB Sensor Generating a Video Stream from Reflected Wavelengths through a Wall (From: Herzig).

### 3. Information Dissemination

Link-16 and other technologies are currently in use to transmit data between platforms and forces (Figure 12) (Fenton, 1999).

- **Conclusion:** The technology exists for a reliable, secure information medium to pass information solutions from sensor to shooter.

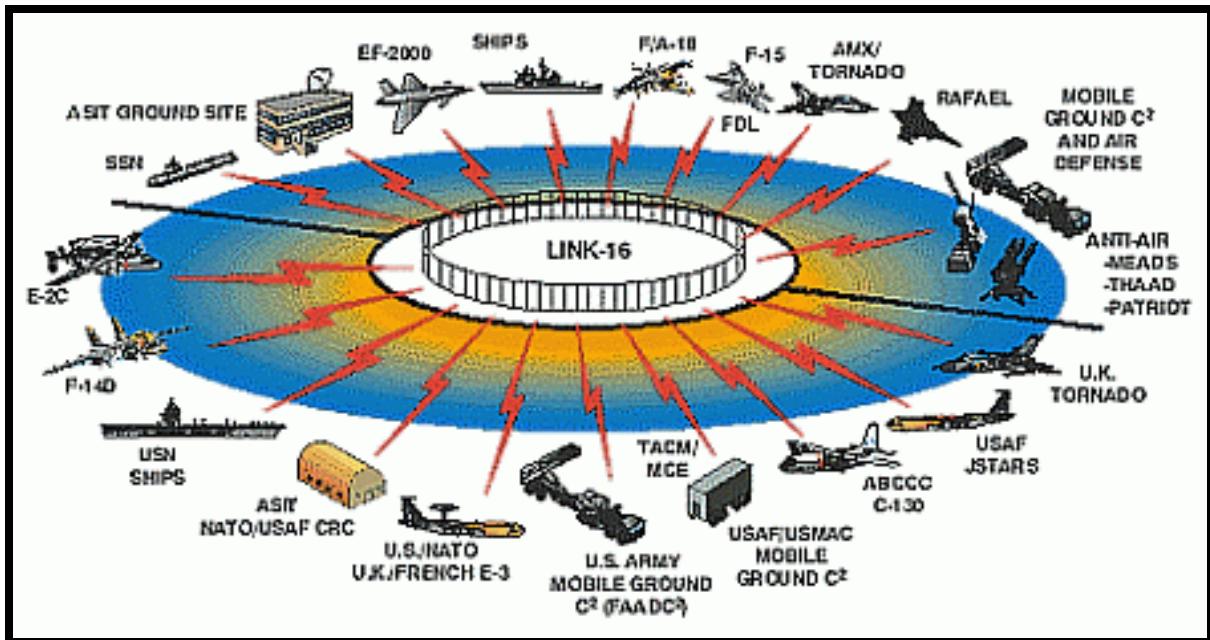


Figure 12. Illustration of Link-16 Interoperability

#### 4. Wireless Information Security

NSA approved SecNet 11 technology exists for 802.11 wireless security at the secret level (see Figure 13).

- **Conclusion:** The technology exists to support of wireless security in a combat zone.



Figure 13. SecNet 11 NSA Approved Encryption

##### **5. Aerially Deployed Autonomous Sensor-Shooter Grid**

The CBU-97/CBU-105 Sensor Fuzed Weapon is an aerially deployed weapon that deploys munitions that hunt with IR sensors, hover, and fire munitions into tanks.

- **Conclusion:** The ability to aerially deploy and maneuver sensors in an optimized grid to autonomously search for and destroy tanks exists. We have a real-time unmanned sensor-shooter grid (Figure 14).

## **Sensor Fused Weapon CBU-97**

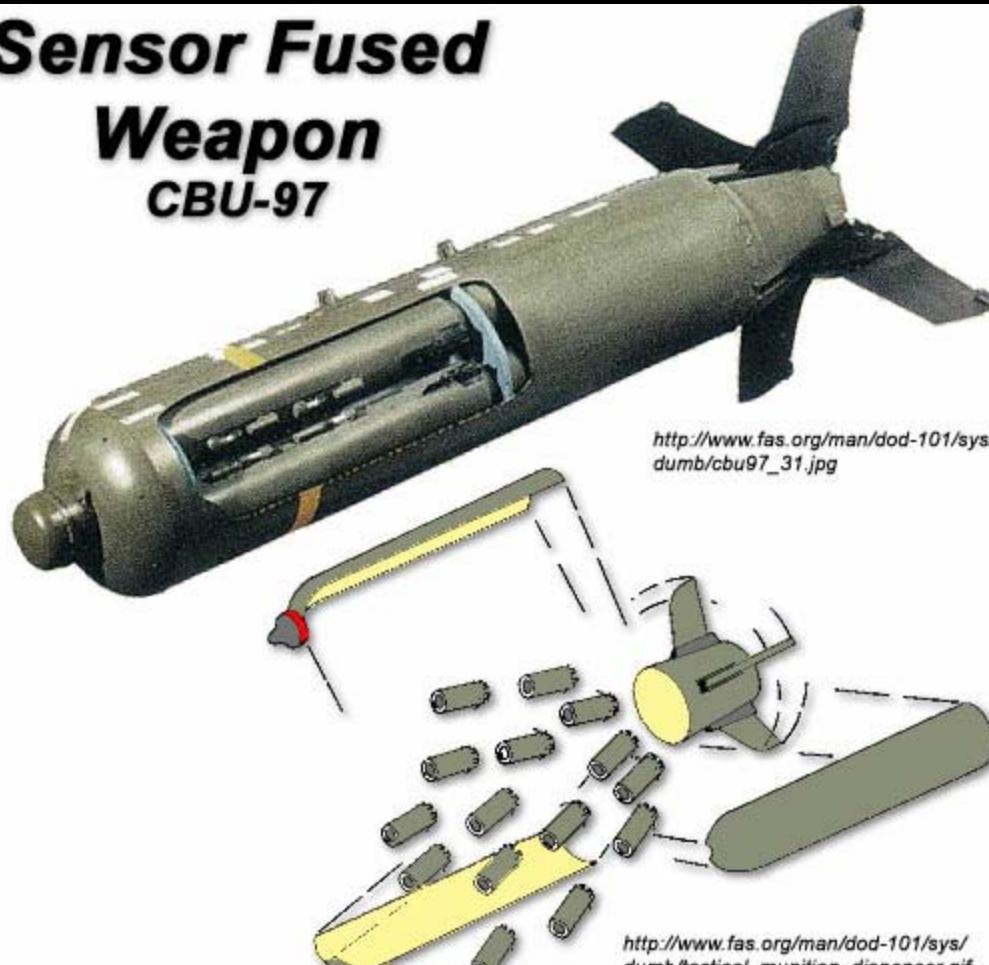


Figure 14. CBU-97 Sensor Fuzed Weapon

### **6. Wireless Mesh Communications Nodes**

MeshDynamics has created COTS technology for a self contained wireless mesh communications network made from numerous self-organizing wireless mesh routing boxes (Figure 15) (Werner-Allen, Swieskowski, & Welsh, 2005; Turon, Horton, Hill, & Broad, 2005).

- **Conclusion:** The technology exists for a self-organizing rapidly deployable hastily formed transmission medium.



Figure 15. Mesh Dynamics Wireless Mesh Box

#### **7. Aerially Deployed Environmental Remote Sensors**

Technology deployed aerially which transmits surface environmental data to an aircraft for High Altitude High Opening (HAHO) and High Altitude Low Opening (HALO) drop accuracy exists.

- **Conclusion:** Capabilities exist to aerially deploy sensors in high tempo operations.
- **Conclusion:** Capabilities exist for the ruggedization of sensors.

#### **8. Remote Power Source Technology**

There is COTS technology to remotely deploy solar powered remote renewable hydrogen power sources. These power sources can be miniaturized and ruggedized (Figure 16).

- **Conclusion:** There exist resources for a sustainable, renewable, and ruggedized remotely managed power source.



Figure 16. Gridpoint Remotely Managed Renewable Power Source

#### **9. Miniaturized Sensor Webs**

The National Oceanic and Atmospheric Administration (NOAA) and the National Aeronautics and Space Association (NASA) have jointly developed a technology labeled *Sensor Webs* designed as a web of adaptive, self healing, miniaturized pods that share environmental information (Figure 17 and 18).

- **Conclusion:** The technology exists for a web of networked, wireless, sustainable, spatially distributed, miniaturized sensors.

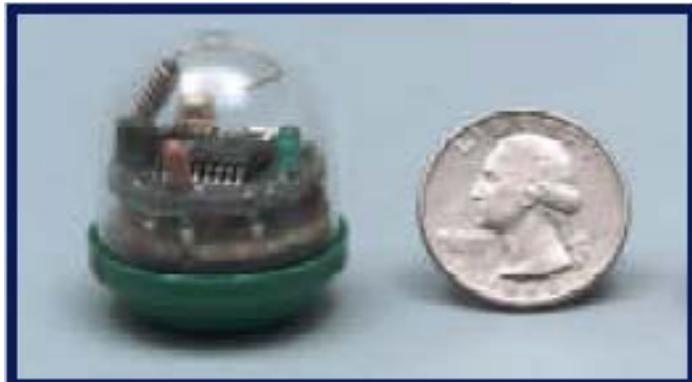


Figure 17. Webbed Pods Created by NASA and NOAA in "The Link Project"



Figure 18. Gumball Size Wireless Sensor Pod

#### **10. Target Data Layered onto a Sensor Feed**

In the British Subway there exists technology to overlay ultra wideband (UWB) sensor data onto a video stream from a camera to identify those carrying firearms or explosives onto the subway.

- **Conclusion:** The technology exists to classify targets as hostile based on what they are carrying, and discriminate between multiple targets.

## **11. Networkable Aerial Sensors**

Rotomotion LLC and Cyberdefense Inc. have both developed networkable miniature unmanned aerial vehicles (UAV's) utilizing 802.11 wireless protocol. These are the CyberBug and the Rotomotion SR50. This researcher was trained to operate both miniature UAV's while supporting the COASTS team in Thailand (Figures 19 and 20).

- **Conclusion:** Mobile aerial sensors exist. Although the prototypes had technical and operational problems, they supported incorporation of mobile aerial wireless sensors into the real-time targeting sensor loop in order to produce the required targeting outputs.



Figure 19. Large Sized CyberBug Launch



Figure 20. Networked VTOL Mobile Aerial Sensor

## 12. Static Aerial Sensor and Transmission Nodes

During COASTS' development of a tactical sensor net tethered balloons were utilized to carry a payload including an internet protocol (IP) camera and a MeshDynamic's routing box attached to them as a payload. The balloons operated effectively as sensor and transmission medium nodes at altitudes up to 4,000 feet (see Figure 21 below).

- **Conclusion:** It is feasible to utilize COTS technology to create an aerial sensor and communications set held aloft by a balloon. As an information medium this provides extended range and could provide a link to additional sensor nets or weapons elements.



Figure 21. Visual Sensor and Information Node

### **13. Summary**

From these examples it is reasonable to conclude that sensor technology and doctrine is in fact gapped far behind the potential capabilities to satisfy current operational needs.

## **C. SENSOR REVIEW**

### **1. Ultra-Wideband Sensors**

According to Herzog (2005) in his analysis of the ultra wideband (UWB) and mesh network technology in the feasibility of UWB sensors for tactical operations, UWB can

operate effectively as a security fence. It can establish a stationary radio frequency perimeter. In addition, due to its wide frequency spectrum and the different ways unique frequencies reflect off of different materials, the UWB sensor system has the ability to discriminate between materials to the resolution of telling a man from a deer, or the location of a firearm on a man's body (Cravotta, 2002; Intel, 2004; Nekoogar, 2005).

Herzig's (2005) work characterizes the UWB sensors in work by Lawrence Livermore National Laboratories (LLNL) as covert. Their signal is difficult to detect since it falls below the typical noise threshold at most distances and has a low probability of intercept (LPI). The pulse-repetition frequency (PRF) is random, mimicking white-noise (Figure 22).

UWB signals act as a reflecting form of radar. In addition they can be used to encode the information necessary for communications and this is another positive attribute for sensor nodes that must communicate, self organize, and finally output information to the weapons actor (Figure 23).

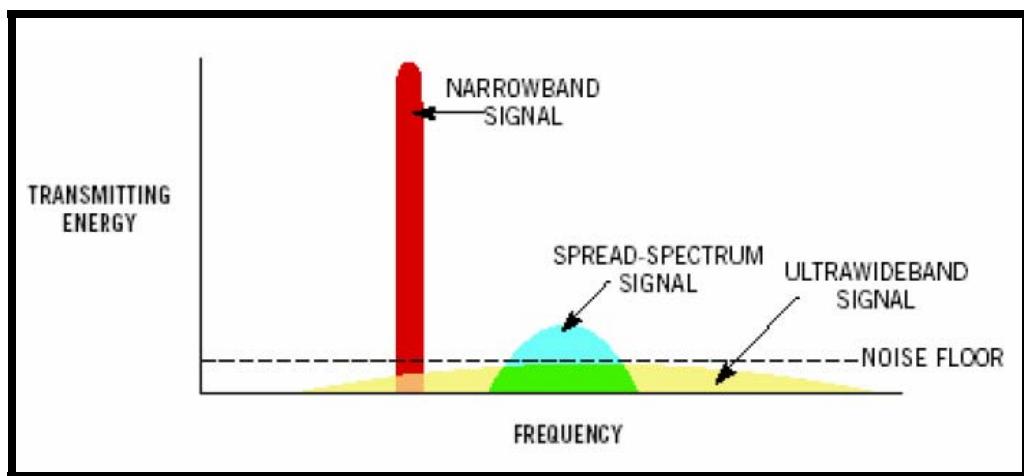


Figure 22. Signal Comparison against Noise Threshold



Figure 23. Full Duplex Handheld UWB Transceiver

In addition, UWB technology can be used for effective geolocation (Figure 24) where coordinates can not be derived from the Global Positioning System (GPS) such as in thick forests or man made structures (Rabaey, Ammer, da Silva, Patel, & Roundy, 2000; Wilson, 2002).



Figure 24. UWB Precision Geolocation System Transceiver

Herzig (2005) also concluded that UWB was the ideal medium for the physical layer of network operations. Coupled with the capability to detect, classify, and output targeting data, UWB provides a multi-use technology that could simplify sensor operations while combining the sensor and the transmission medium into the same node (Callaway, 2004; He, Stankovic, Lu, & Abdelzaher, 2003).

These capabilities combined with LLNL developed UWB technology for military applications makes it the leading candidate sensor for full spectrum coverage of target reflections (Herzig 2005). The capabilities of UWB allow for autonomous characterization of targets (Cravotta, 2002).

In addition, LLNL is currently researching and producing a device titled the "Guardian Sensor" which is an UWB device also that also acts as a sensor fence.

## **2. Visual Feed Sensors**

According to a recent report by Innovative Wireless Technologies (2006), improved communications and awareness of one's situation are vital components to reaching current military objectives both at home and overseas. "A key aspect...is sensor networks. These sensors, with ad-hoc networking capability, could provide an early-threat detection that is rapidly deployable, failsafe and inexpensive" (p. 1).

Visual sensors or sensors that can produce a visual output from emissions or reflections (IR, near IR, UWB, or even acoustic) are also essential in a sensor net that will create a real time sensor-loop for command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) (DeBardelaben, 2003; Fraden, 2004).

#### **D. CHAPTER SUMMARY**

The purpose of this chapter was to review literature pertinent to the study. The first section described the new form of warfare. It was explained that victory has been redefined as the spread of the correct ideology to prevent the tasking of the attack on the U.S. or her interests by individuals capable of it.

Technologies and sensors were reviewed next. The review included discussion on ultra-wideband and visual sensors. The following portion of the review focused on problems with research. COASTS and Thailand problems were detailed, followed by an examination of general real-time targeting issues. Included were discussions of small shooter-small sensor, COASTS deployment, and sensor net operations.

Chapters I and II of this thesis have now laid the groundwork for the study and its attendant objectives. The following chapters will now define the problem and develop a model for the solution.

## **IV. MODEL ANALYSIS**

The purpose of this chapter is to describe the model recommended for resolving the TDG problem. Before this can be achieved, however, it is first necessary to explain need and define requirements. Following that will be a description of solutions and the model architecture.

### **A. NEED**

The need for real-time targeting solutions in the uncontrolled OE regions of Thailand is representative of the global need the U.S. must meet in the GWOT.

#### **1. Need in Thailand**

The need for successful operations in Thailand has never been greater. Asymmetric threats to the national security of America continue to increase (Parr, 2003). These include narcotics smuggling, piracy, human trafficking, and terrorism, among other similar activities (Parr, 2003). Globalization of these types of activities continues to redirect American attention away from her own borders. In addition, the separatist insurgency in the southern provinces has been linked to various terrorist organizations that operate internationally and have been a serious threat to not just Thailand, but to the United States and its allies as well (Roberts, Trace, & Klein, 2004).

Unfortunately, current tactical systems are not able to rapidly deploy a common information environment among air and land entities. An autonomous network cannot be generated. While some technologies exist that could assist

in this endeavor, these typically do not meet the stringent DoD and coalition partner requirements for the GWOT and other security missions.

Security issues now command the fullest attention. These are being addressed on many different levels. For example, Joint Interagency Task Force West (JIATF-W) is initiating data/intelligence fusion centers in Chiang Mai, Thailand. Such a data center focuses on collecting intelligence for many different types of operations. In addition, the Regional Maritime Security Initiative (RMSI) is focusing on coastal areas involving transnational open ocean counter-piracy and counter-terrorism.

These entities are now meshing their activities with American efforts in a coalition-oriented effort to decrease the ever-growing problems associated with illegal drug activities and human trafficking (Roberts et al., 2004). The growth of such problems was recently reported by the Bangkok Post (03 January 2006) as follows:

The [Thai] Narcotics Control Board forecasts a continuing rise in the number of drug-related cases this year, but expects the overall amount of methamphetamine in circulation to decline. Secretary-general Krissana Polanant said the trend is for traffickers to carry smaller quantities of pills which means the smugglers will have to make more trips which increases the chances of them being arrested. Provinces on the bureau's close-watch list are Chiang Rai, Chiang Mai, Tak, Nan, Nakhon Sawan, Nonthaburi, Sing Buri, Ayutthaya, Nakhon Pathom and Bangkok.

## **2. Perceived Thai Problem**

According to a recent report (Central Intelligence Agency, 2005), Thailand has an extended border with Burma that requires military assets to patrol for the purpose of

battling drug smugglers and human traffickers. The military provides monitoring, surveillance, and targeting. The illicit drug smuggling and trafficking in human cargo has significantly increased in recent years and has become a significant problem, especially in light of the fact that these illicit operations can provide financial support for international terrorist organizations. The problem is further increased when note is taken that many of the illegal drugs reach the United States through shipments through the Straits of Malacca and Singapore Straits. It is the responsibility of the Royal Thai Army (RTA) 3rd Army to maintain ground-based security and surveillance.

Other security problems are currently occurring which demand Thai military attention in the southern regions of Thailand. In fact, the RTA 4th Army has been deployed to this region to deescalate tensions caused by insurgency and unrest.

In addition, small boat activity in the Gulf of Thailand has escalated. The purpose of this activity is to illegally distribute weapons and ammunition. All these problems and insurgencies have financially impacted the Thailand government and taken their toll on the country's military forces. Clearly, more capable ISR will enable Thailand to reduce asymmetric attacks against civilian and military targets.

### **3. COASTS Scenario Overview**

The COASTS research team executed a drug interdiction scenario (see Appendix C for details on the COASTS concept of operations) in direct support of the following nine principal mission areas. These are briefly described as follows (*COASTS Thailand Field Experiment, 2006*):

1. Direct Action (DA): During short-duration, high-tempo offensive missions, the primary function of COASTS is to provide force protection that requires little or no operator interface. COASTS also will provide automated reporting to the Tactical Operations Center (TOC) for potential threats relevant to a specific mission.

2. Tactical Reconnaissance (TR): The purpose of a TR mission is to collect data. COASTS will augment other capabilities to obtain/verify information and will support a range of information and communication functions.

3. Foreign Internal Defense (FID): COASTS assists Host Nation (HN) military and paramilitary forces, with the goal to enable forces to maintain the HN's internal stability.

4. Combating Terrorism (CBT): COASTS will support CBT activities to include anti-terrorism (defensive measures taken to reduce vulnerability) and counterterrorism (offensive measures taken to prevent, deter, and respond).

5. Civil Affairs (CA): COASTS assists in peacetime to preclude grievances from flaring into war and during hostilities to help ensure that civilians do not interfere with operations and that they are protected.

6. Counter-proliferation Weapons of Mass Destruction (WMD): COASTS assists traditional capabilities to seize, capture, destroy, render safe, or recover WMD. COASTS also provides data to assist U.S. military forces and coalition partners to operate against threats.

7. Information/Counter-Narcotic Operations: COASTS augments actions and applies information across all phases of an operation and the spectrum of military operations.

Counter-narcotic operations augment JIATF-W, U.S. Embassy Bangkok, and Thai law enforcement efforts to reduce the level of transnational narcotic smuggling.

8. Maritime Security and Interdiction Operation: COASTS uses C4ISR capability for small boats capable of conducting maritime terrorism exclusion operations. The modular usage of fly away kit (FLAK) technology makes small boat interdictions ISR-mission capable. Visit, board, search, and seizure (VBSS) operations are conducted by all U.S. and coalition forces.

9. Psychological Operations (PSYOP): As a vital IO tool in counter-insurgency and counter-terrorism operations, the COASTS research program analyzes the ability of the wireless network to be utilized for PSYOP missions in the tactical environment.

#### **4. COASTS Scenario Overview**

The scenario decomposed the force into its component parts and highlights the redefinition of the component parts of military actions. It should be noted that three fundamental classes exist in this object orientated operation. These include: sensor, information input/output, and the weapons action.

Illustrated below in Figure 25 is a visual representation of the scenario.

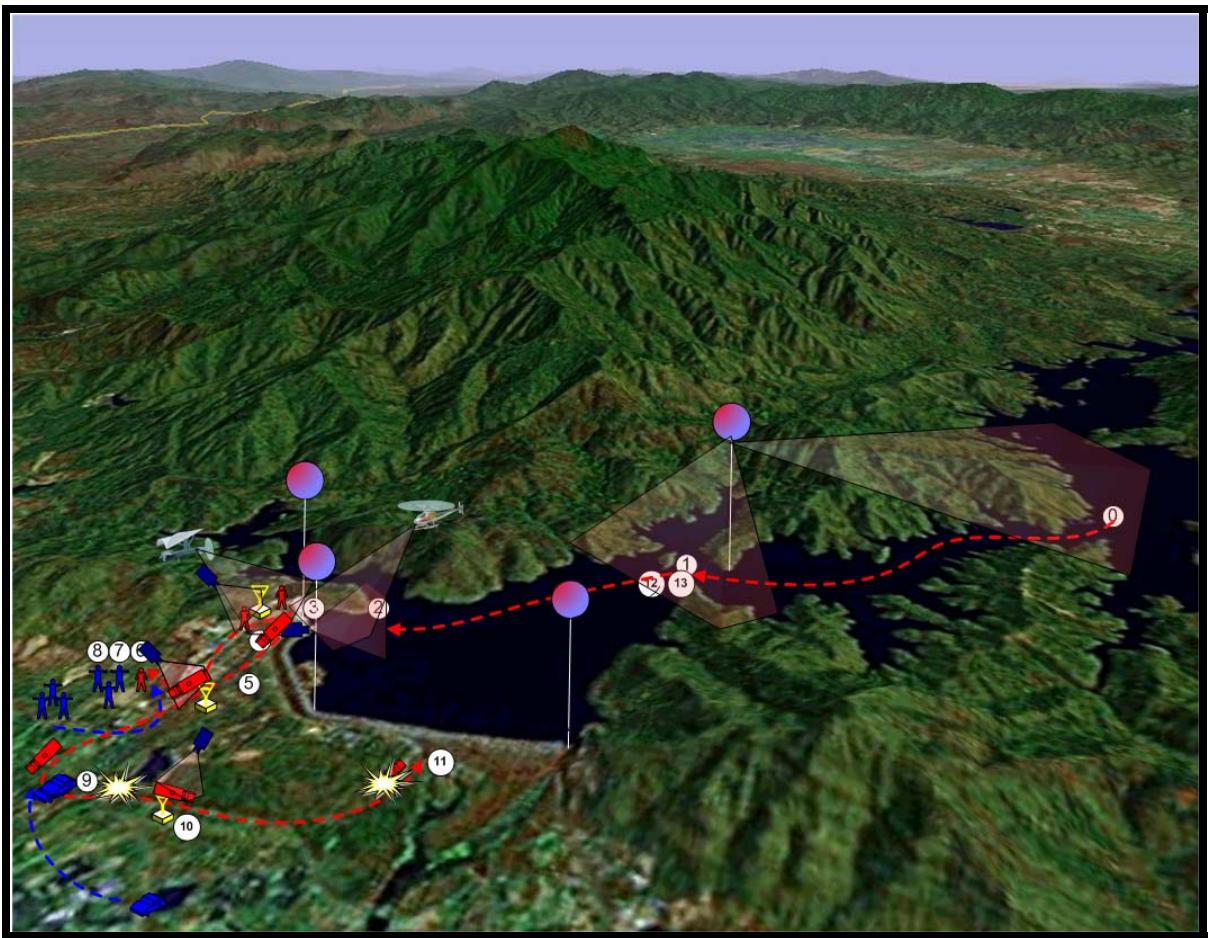


Figure 25. Event Breakdown for the Mae Gnat Dam Drug Interdiction Scenario

During the above functional decomposition of a real-time targeting force, three broad classes of action were developed:

1. Sensor Operations: for identification, classification, and location of target(s);
2. Information Transfer: for transfer of above processed information through the information medium.
3. Weapons Action: takedown or destruction of identified targets—this doctrine has been developed and well refined through military history.

The Weapons Action portion of the operation is ready to receive inputs from targeting. However there is little doctrine for iterative real-time targeting.

#### **B. REAL-TIME TARGETING PARADIGM PROBLEM**

Special forces (SF) end-users when regarding targeting operations assumed that a paradigm existed for real-time targeting. What was found, however, was that in reality very little of the real-time targeting paradigm existed in the collective consciousness of the Special Forces. Instead, personnel were focused on targeting as a non real-time process. Little or no focus was paid to enhancing capability. Instead, it was insinuated that the sensory operations for most missions followed naturally from the doctrine sensor information came from visual human ground sensors, visual human aerial sensors, etc. Data would be passed over a voice net between sensor and shooter and often the sensor was the shooter. The enhancement and separation of the sensor element was not regarded as a principle of warfare.

#### **C. SENSORS**

##### **1. Small Shooter-Small Sensor**

Today's sensors have too much footprint. But there is almost no footprint for shooters up at 30,000 feet against GWOT enemies. Clearly, sensor operations require improvement. How should this be fixed? Doctrine and sensor technology for past conflicts with a larger level of bounded combat exists. Previous doctrine required the forces to be bounded in geography, communications,

movements, and tactics. Such bounding of forces is an assumption of a previous form of warfare that no longer holds true.

As previously noted, victory has been redefined by the enemy. No longer is it a national victory; rather, it is ideological. Because of the nature of the forces – that is, independently operating cells – and the nature of their goals (political) the American military force faces a changing combat paradigm. Because the luxury of detecting division level forces no longer exists, shooters have been adjusted appropriately. However, the sensors continue to struggle. A current solution for this lagging sensor technology is often heard in the common rhetoric of "boots on the ground." In other words, people need to be sent in to walk around and visually identify targets and produce from that visual identification a location-relative or absolute—and then follow with the necessary operations to prosecute targets at that location. Consequently, the sensors (humans in this case) that are employed are limited conceptually, technologically, and doctrinally.

Because of these changing requirements and assumptions the principles of warfare have shifted from what they once were. There is little focus upon where to direct combat power and little focus on sensor necessity. Figure 26 highlights the currently recognized principles of war.

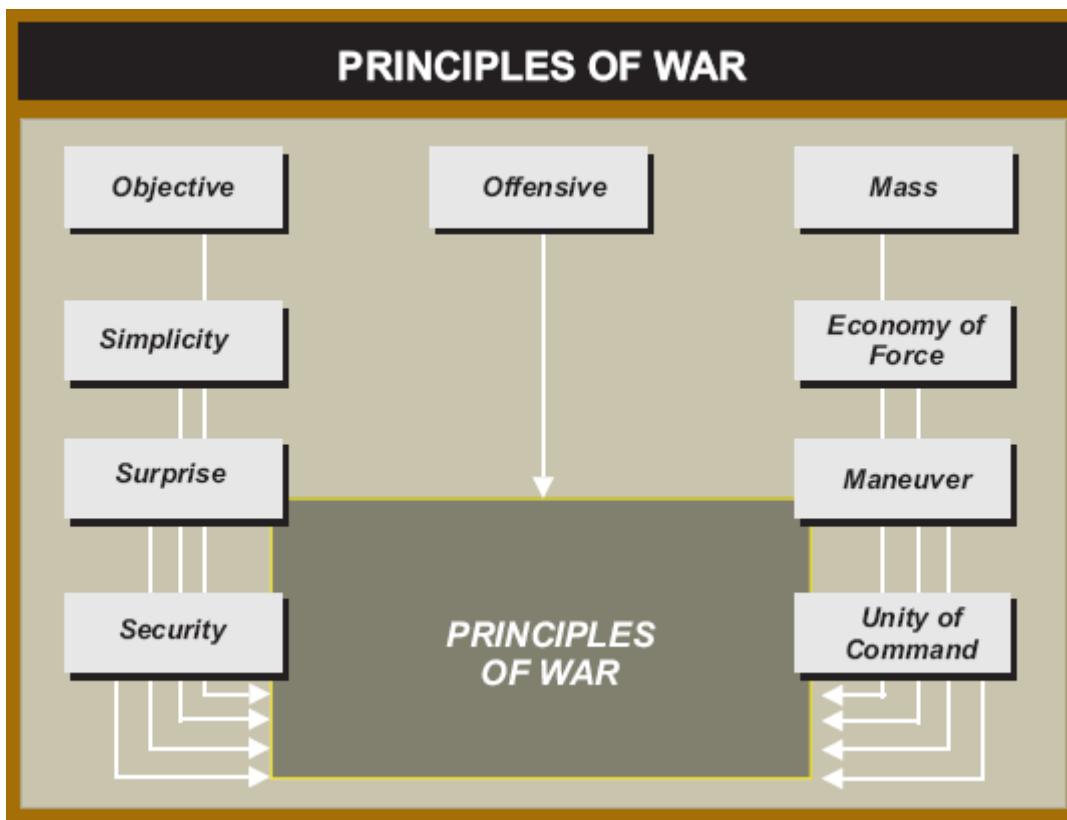


Figure 26. Current Recognized Principles of War

Figure 27 illustrates the real-time sensor cycle<sup>1</sup>, today's technology has enabled the medium that binds the shooter to the sensor. Bootstrapping has focused the majority of concern on the shooter because in the past the opposing forces have not been difficult to detect - at least not with the level of technology that existed at the time. Thus, sensors have been shooters.

---

<sup>1</sup> See Lim (2001) for information dissemination in self-organizing real-time sensor networks.

## Real-Time Sensor Cycle

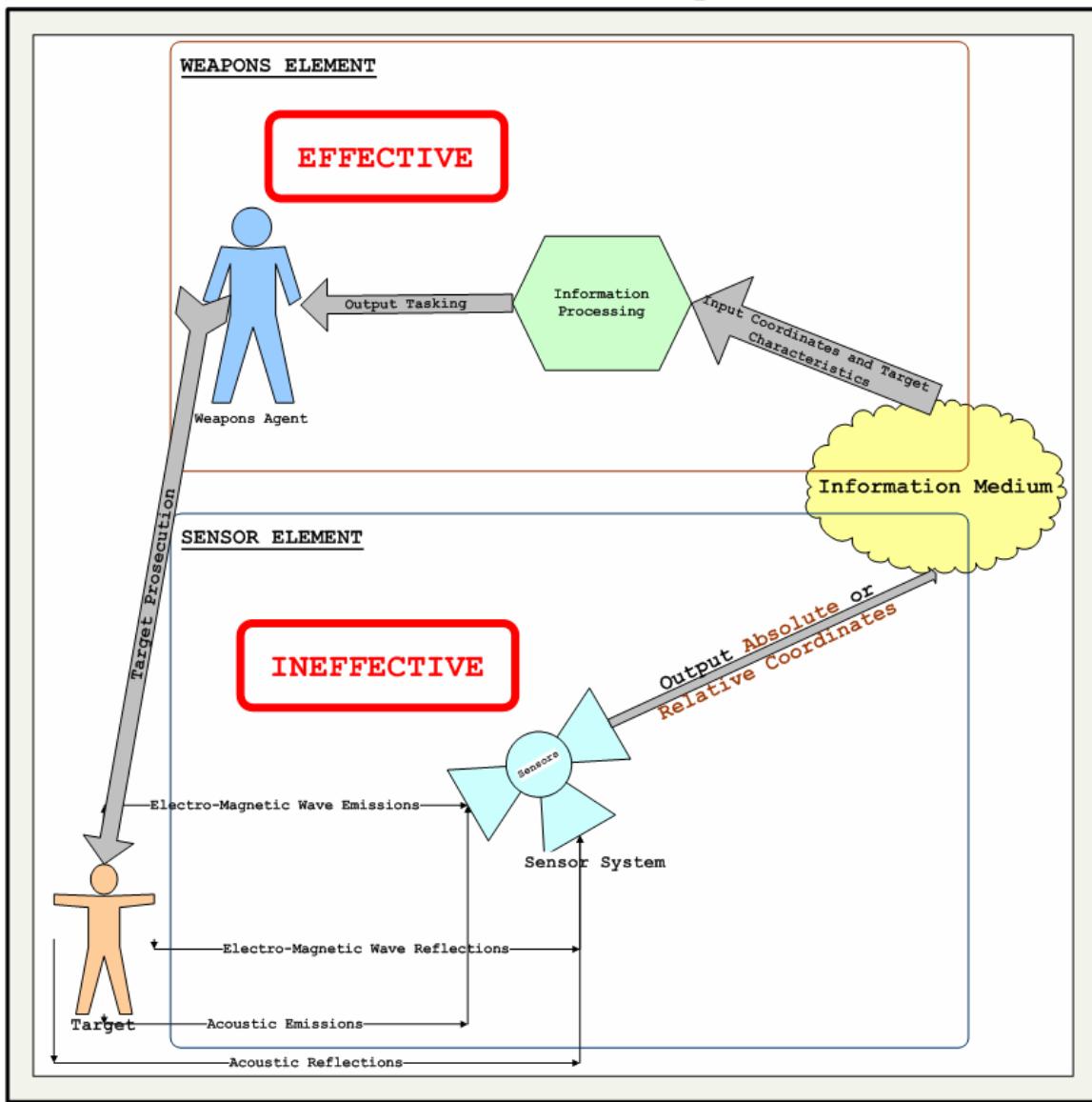


Figure 27. The Real-Time Sensor Cycle

As can be seen in the Figure 28, the task of targeting is not focused upon in the current Joint Architecture for joint special operations task force elements. Architecture is not broken down along functional lines; instead it is broken down into traditional task oriented components. The proposed real-time targeting architecture suggested in this thesis is broken down into elements that are functionally

separated into sensor, information processing, dissemination, and prosecution elements. These elements could be automated and do not necessarily require humans in the loop.

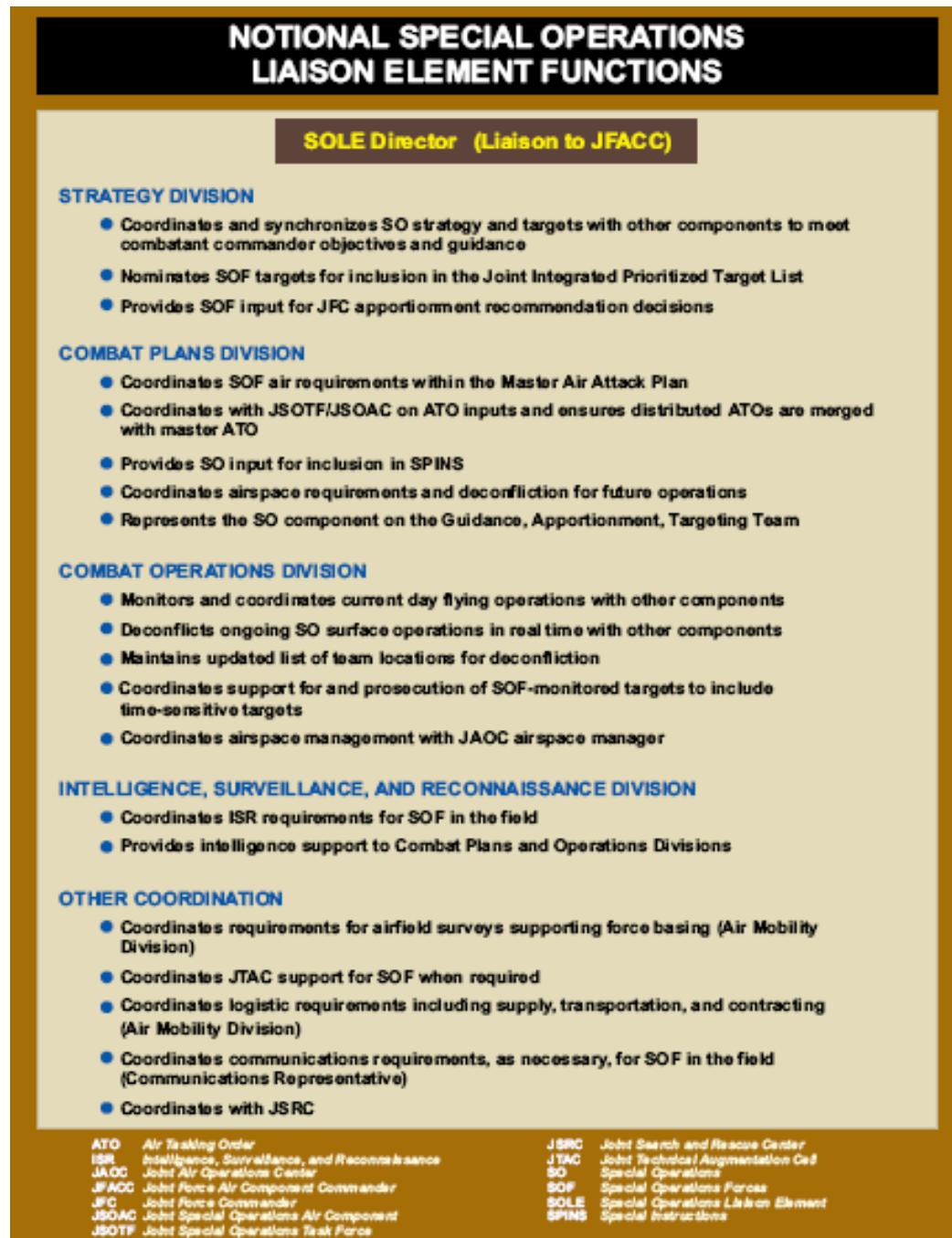


Figure 28. Special Operations Liaison Element Functions  
(From: JSOTF Pub)

## 2. Sensor Net Operations

The C4ISR operators require several objects layered with the sensor feed to utilize it for situational awareness (SA). The first is visually represented positional data, most likely a map or an overhead image with an updating overlay of the field of view (FOV) (Figure 29). The second is simplified target classification data layered onto the feed(s). Target classification, for example, could include an overlay onto the real time feed identifying the target with a rendered box (Figure 30). The target can then be identified on the feed and mapped to the common operational picture. Otherwise, in a congested local area of operations, the target will be lost in the noise.

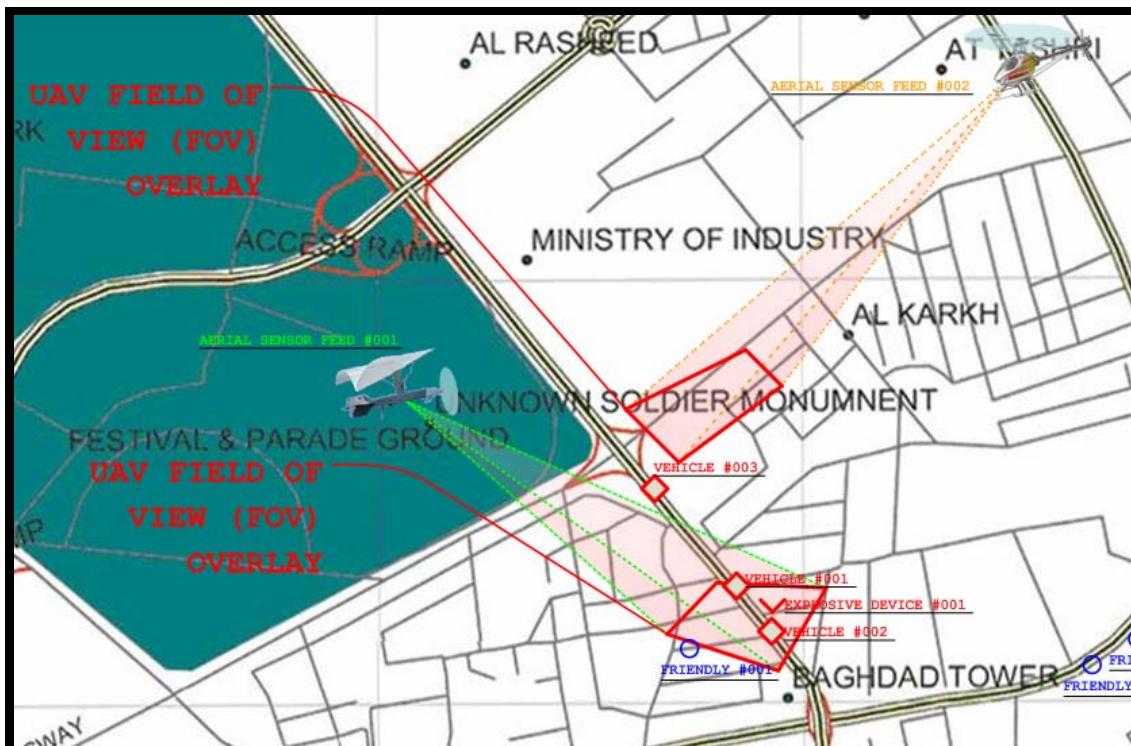


Figure 29. Common Operational Picture Displaying UAV Sensor Feed FOVs, TDD, and Friendly Overlay

In addition, sensor feed overlays should take advantage of UWB capabilities by indicating hostile equipment or contraband (improvised explosive devices (IED's), firearms, etc.) on persons or targets. Finally, not included in the feed, but in the feed interface, there must be some way of identifying and accessing multiple feeds for the operator. There must be a portal interface that prioritizes which feeds provide the most targeting information on the COP.

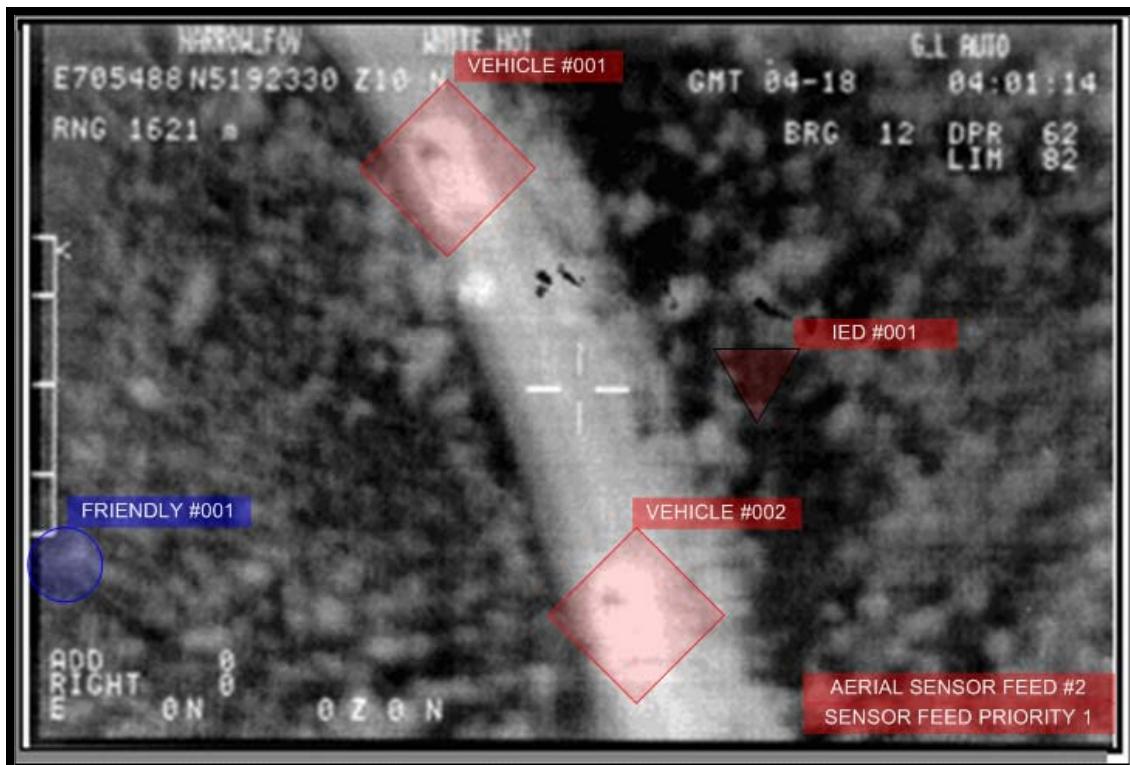


Figure 30. Aerial Sensor Feed Overlaid with TDD, Friendly Data, and Sensor Feed Priority

In experiences with UAV operations and sensor net operations, it was found that SA was not generated adequately from a raw visual feed (Yan & Tsa, 2005). Instead, the feed required SA augmentation. This augmentation takes the form of an overhead or map display

with the FOV rendered on it in real-time. This gives the client of the sensor net adequate SA to transform a raw feed into actionable knowledge.

In precision guided bomb procedures the process is similar with the airborne operator guiding in the bomb based on a visual reference produced from SA, from a map or a visual look. In addition RQ-1 Predator drones utilize this exact FOV mapping method, calculating the location of the FOV from laser range data.

In experiences with airborne visual sensor feeds (CyberDefense's Cyberbug, Rotomotion vertical takeoff and landing (VTOL) UAV's) without an accompanying geographical orientation rendered, it was difficult to identify the location of practice targets. To gain the SA required, frequent camera orientation to the front of the aircraft (swiveling it up to a forward looking view) and correlating it with the direction of flight displayed on the map the ground control station displayed for navigation purposes (Figure 31) was required. If the sensor is providing an SA feed, the process needs to be appropriately formalized for mobile airborne sensor operations.



Figure 31. CyberDefense CyberBug Gimbaled Visual Sensor Feed

#### D. END-USER SURVEY

##### 1. Problem Definition

The largest problems for operators attempting to prosecute targets within OE's are: (1) target discrimination between the non-combatants and enemy targets and (2) opaque barriers obscuring targets such as the jungle environment foliage or man made structures. This is because insurgents are often embedded within the local populace. The main problem is the variation of environmental opacity obscuring sensor capability in addition to the discrimination of actual targets and non-combatants. The margin for error is small making this a difficult problem. Within such OE's where Joint forces are operating, the fog of war becomes an issue with friendly SA causing fratricide.

##### 2. Discrete Deliverables

There are several discrete deliverables required from sensor operations to input into weapons operations as defined by the end-user survey. These are:

- Highly accurate grid coordinates in Military Grid Reference System (MGRS) format (most sensor systems deliver a general location of sighted warm bodies which is often not sufficient for targeting)
- SA feeds augmented with grid coordinates
- Information on whether targets are armed or unarmed
- Accurate numbers of personnel
- Queuing of targets in prioritized by threat
- Proper fusion of the sensor data
- Generation of an accurate, COP
- Secure and reliable transmission of the COP

### **3. Ideal Equipment Requirements**

On the tactical level ground sensors that can provide real-time sensor feeds equivalent to that of Human Intelligence (HUMINT) or equivalent to that of an RQ-11 Raven UAV (Figure 32).



Figure 32. RQ-11 Raven Squad Level UAV

On the operational level a wide area of coverage must be kept within an SA feed to provide operators with the SA of their larger operational surroundings equivalent to that of a RQ-1 Predator (Figure 33).

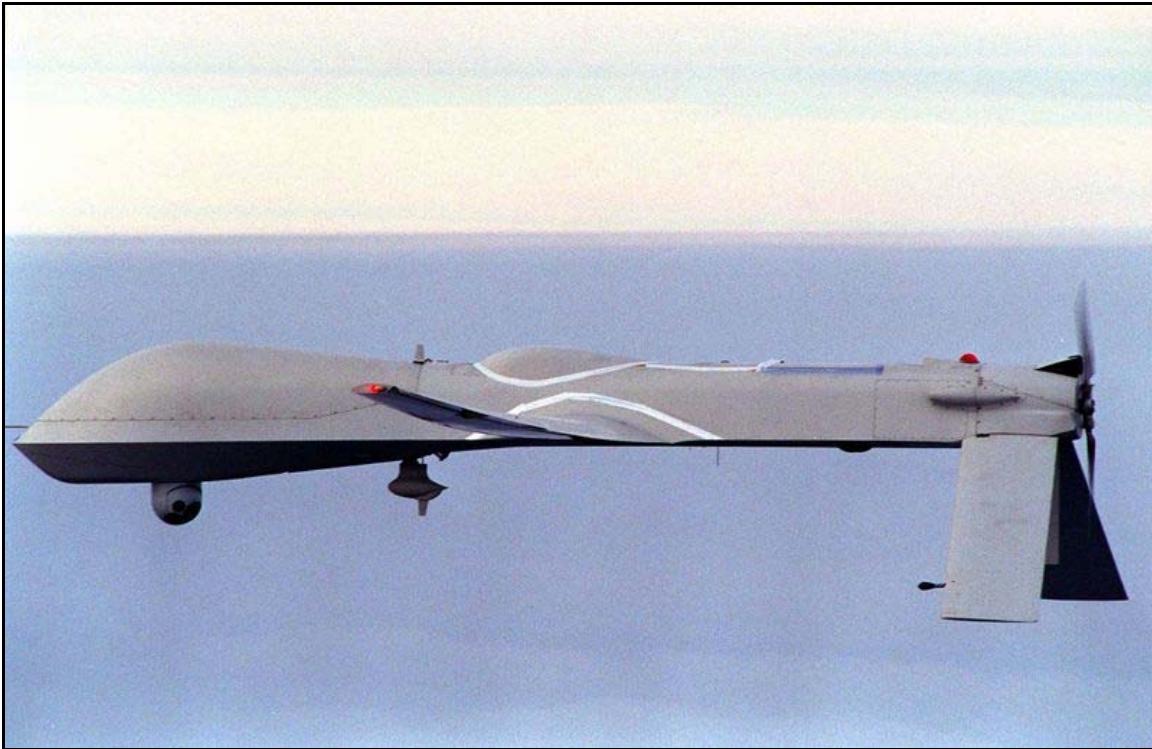


Figure 33. RQ-1 Predator UAV

#### **4. Ideal Doctrinal Requirements**

Doctrine must support a policy of bootstrapping and empowerment of the scene operators responsible for target prosecution. That is the primary mission. The data must be simple and feed directly to the operator. There should be no middle-man utilizing the data to manage the operators. The on-scene operators must have supreme control over their incoming data to produce the desired weapons effect.

Mission modularity is key. The On-Scene commander must be empowered to tailor the mission, equipment, and personnel in modular building blocks to the appropriate mission. Also, personnel footprint should be minimized.

## **E. MEASURES OF EFFECTIVENESS ANALYSIS**

A list of important considerations can be found in Appendix A. This section now provides MOE answers. Each MOE is listed first, followed by a listing of component parts and answers:

1. Target Discrimination
  - a. Equipment - Utilize Ultra Wideband (UWB) frequency patterns to recognize hostile equipment
  - b. Location - Locate target with any sensor available, output a grid-coordinate layered with target data
  - c. Stance - Requires a sensor to visual real-time feed for screening by a human operator to discern hostile stance, layer in additional sensor data.
  - d. Target discrimination data must be stored and correlated in a database in order to maintain target fidelity should the target move out of range of UWB sensors and into larger range passive sensors
  - e. Suggested Equipment - IR/Near IR Sensors/Visual Sensors
2. Grid Coordinates
  - a. Visual, IR, Near IR, or even acoustic based sensors can passively acquire a set of targets. In addition, active acoustic sensors could be utilized to locate targets. However, such sensors will need target discrimination data layered on top of the coordinate outputs. The larger set of targets can be filtered with UWB active reflection data to discriminate hostile targets. With positional data either from UWB device geospatial orientation, or a global positioning system (GPS) output meshed with range data to a device's known position targets can be localized.

3. Real-Time Visual Stream
  - a. A real time visual stream can be produced from IR, Near IR, or even UWB Sensors. Real-time feeds from UWB type sensors have the added advantage of penetrating through opaque environments. Again the output must be layered with Target Discriminating Data (TDD) for the operator interface. Real time feeds can come from ground sensors, however the most effective sensor for maintaining a passive IR/Near IR/Visual feed is a mobile or static aerial sensor.
4. Prioritization of Sensor Feeds
  - a. Accomplished through autonomous software analysis of UWB TDD on such variables as hostile equipment, number of hostile targets, and high priority locations of targets. In addition, manual input by operators of high priority targets prioritized by stance or otherwise should override autonomous settings.
5. Queuing of Targets
  - a. Process similar to Prioritization of sensor feeds. Targets will be queued with layered UWB TDD in addition to operator overrides.
6. Layered COP
  - a. Layered COP will be generated through complete sensor fusion onsite within the payload of a persistent aerial sensor onboard a payload onboard a tethered static aerial sensor. This portion of the system should be highly redundant as it is fault point. Tethered Static Unmanned Aerial Nodes should be equipped with payloads capable of autonomous sensor fusion operations to support prioritization, queuing, and layering of data. In addition these airborne fusion centers should be the centers for layering of sensor feeds to support the operator. Finally, the payloads should also carry a backhaul transmission to a forward operating base (FOB), airborne platform, or other gateway outside of the local operating area.

## 7. Dissemination of Data

- a. Backhaul gateways will disseminate data beyond the sensor net. The gateways will be contained onboard static aerial nodes. These static aerial nodes could either be a tethered balloon or a persistent airship. The payloads must be compatible with a number of different transmission mediums including but not limited to UHF, SATCOM, and Link-16 in order to deliver end products to weapons delivery systems such Tomahawk Land Attack Missiles or Attack Aircraft. In addition, the common operating picture can be provided upwards to higher levels for dissemination to commanders for support operations.
- b. Within the sensor net, ground operators can interface directly with client devices. Transmission nodes will utilize UWB as the physical layer of communication for the transmission medium since it is the most secure and robust for operations in opaque environments.

## 8. Ground Operator Interface

- a. Ground operators within the operating area should have access to the autonomously filtered TDD, prioritized sensor feeds for SA, and targeting solutions via a rendered common operational picture. The interface will be wearable, possibly a heads up display (HUD) helmet (not unlike S.W.A.T. helmets or the HUD Helmet in development for the F-35 Joint Strike Fighter) or a wearable device preferably on the forearm. The device must utilize a full spectrum interface that can accept voice and keyed commands. All methods of end-user experimentation and survey should be utilized to find out the optimal method for the man-machine interface. The data deliverable to the ground operators within the sensor net will include (1) a COP in the form of a map with layered targets on top of it. The TDD on each target should be hidden but accessible through the graphical user

interface (GUI) layers for the operator. In addition, real-time sensor feeds should be available to the operator in a prioritized fashion with FOV selection. If there are airborne mobile sensors the operator should have access to control their FOV coordinates.

#### 9. Rapidly Deployable

a. Airborne deployment of the system is necessary for sensor net operations. It is the only foreseeable solution to high tempo operations requiring a sensor net. The sensor net should be deployed from an aircraft, or several aircraft. The deployment design should conform to the terrain of operations. For instance, if operating within triple canopy jungle UWB sensors should be deployed from aircraft via a parachute system that will entangle them and have them looking downward from the trees. In other terrain sensors could utilize deployment not unlike that of the device used to sense surface environmental data for HALO drops (a device deployed from an aircraft that implants itself by a stake in the ground). The UWB sensors should be deployed in a highly redundant fashion to ensure the fidelity of the net. UWB sensors should be deployed as the primary ground sensor and if they can be ruggedized sufficiently they should be deployed in a cluster fashion similar to that of the SFW. IR, Near IR, and Visual passive sensors will need to be onboard the payloads of static aerial devices since they provide also the majority of wide area coverage. UAV's that mesh with the sensor net should be launched.

#### 10. Modularity

a. System will have preset TDD prioritization algorithms for varying Rules of Engagement (ROE), varying deployment payloads, varying deployment patterns, and varying operating environments.

## 11. Interoperability

- a. System will be interoperable with Link6, UHF/VHF/HF bands, satellite communications (SATCOM) and other transmission mediums required to make the precise passing of targeting data to shooters possible. This capability will be deployed onboard the static aerial sensors to ensure fidelity and access.

While the above provides MOE answers for the new system, it is important to add several important notes:

- Static aerial nodes are required at varying altitudes for persistent aerial real-time feed coverage (recommend up to 4,500').
- Static aerial nodes are also required at varying altitudes for backhaul transmission and wide area transmission coverage/redundancy. This transmission system can also serve as a secure and reliable medium for audio communications. The operator only need transmit to the nearest transmission node and transmission will be relayed through the entire net.
- TDD is required for discriminating Hostile Target Equipment. For example, in Baghdad, IED's are a hostile equipment priority. In Thailand large quantities of narcotic substances are the priority, and in the Philippines, Soviet made weaponry are the priority. This of course, relies upon the final capabilities of UWB discrimination capabilities. Prioritization tables of hostile equipment should be included in the AO modular package. This data helps for queuing and prioritization of targets.

## F. SYSTEM (MODEL) ARCHITECTURE

The system architecture will be broken down areas as follows:

### 1. Sensor Net Elements

#### 1.1. Real-Time Sensor Feeds (can be anything that produces a real-time feed)

##### 1.1.1. Aerial Feeds

1.1.1.1. Mobile Aerial Feeds

1.1.1.1.1. Function:

1.1.1.1.1.1. Flexible Aerial Coverage of Local Operating Area

1.1.1.1.2. Example Equipment:

1.1.1.1.2.1. RQ-11A Raven

1.1.1.1.2.2. RQ-1 Predator

1.1.1.1.2.3. RQ-4A Global Hawk

1.1.1.2. Static Aerial Feeds

1.1.1.2.1. Function:

1.1.1.2.1.1. Persistent Coverage of Wide Area for area coverage a visual type passive sensor, real-time feed

1.1.1.2.2. Example Equipment:

1.1.1.2.2.1. Tethered Balloon Payload Aerial feed (Visual/IR/Near IR)

1.1.2. Ground Feeds

1.1.2.1. Static Ground Feeds

1.1.2.1.1. Function:

1.1.2.1.1.1. SA Augmentation with overlayed FOV and TDD

1.1.2.1.2. Example Equipment:

1.1.2.1.2.1. Ground Passive Visual, IR, or Near IR Camera feeds

1.1.2.1.2.2. UWB Active Sensor Reflections transformed into Visual Sensor Feeds for environmental transparency

1.1.2.2. Mobile Ground Feeds (Manned Sensor Feeds)

1.1.2.2.1. Local Area Operator Sensor Feeds (Visual/IR/Near IR)

1.1.2.2.1.1. Function:

1.1.2.2.1.1.1. Flexible ground SA Augmentation with overlayed FOV and TDD

1.1.2.2.1.2. Example Equipment:

1.1.2.2.1.2.1. Vehicle Mounted Sensor Feeds

- 1.1.2.2.1.2.2. Maritime
- 1.1.2.2.1.2.3. Terrestrial
- 1.1.2.2.1.2.4. Wearable Sensor Feeds

## 1.2. Threshold Sensors

### 1.2.1. Functions:

- 1.2.1.1. Provide Area Target Coverage and area prioritization
- 1.2.1.2. Do not provide sensor feeds, they provide alerts when the threshold of passive emissions is detected for area prioritization

### 1.2.2. Equipment Example:

- 1.2.2.1. Static Aerial Payloads of Magnetic/Acoustic/IR/Near IR/Visual Sensors
- 1.2.2.2. Static Ground Threshold Sensors of Magnetic/Acoustic/IR/Near IR/Visual Sensors similar to the Crossbow sensors utilized in the COASTS 2006 program

## 1.3. Active Friendly Transmitters

### 1.3.1. Functions:

- 1.3.1.1. Transmit location data on friendly units to sensor fusion payloads to provide friendly SA

## 2. Transmission Medium Elements - UWB Physical Layer

### 2.1. Ground Nodes

#### 2.1.1. Mobile

##### 2.1.1.1. Functions:

- 2.1.1.1.1. Provide a flexible SA and data gathering intelligence center if necessary
- 2.1.1.1.2. C2 Functions
- 2.1.1.1.3. Can serve the Gateway function for interoperability purposes
- 2.1.1.1.4. UAV integration/operation

##### 2.1.1.2. Example Equipment:

- 2.1.1.2.1. Network Operation Centers (NOC) similar to the Nemesis Van utilized in COASTS 2006 prototyping at Pt. Sur, Ft. Ord, and Camp Roberts

2.1.1.2.2. Man Portable Transmission Medium  
Nodes similar to the tactical communications  
Kit utilized in COASTS 2006 at Mae Gnat Dam

## 2.1.2. Static

### 2.1.2.1. Functions

2.1.2.1.1. Serve as a reliable Physical Level  
layer for a transmission medium

2.1.2.1.2. Provide communications security  
through frequency hopping

### 2.1.2.2. Example Equipment:

2.1.2.2.1. UWB Nodes (can double as sensors  
and transmission nodes)

## 2.2. Aerial Nodes

### 2.2.1. Mobile

#### 2.2.1.1. Functions

2.2.1.1.1. Flexible Network Extenders

#### 2.2.1.2. Example Equipment

2.2.1.2.1. Predator UAV's acting as network  
extenders

2.2.1.2.2. Rotomotion VTOL Miniature UAV's  
ability to extend a 802.11 Network

### 2.2.2. Static

#### 2.2.2.1. Functions:

2.2.2.1.1. Wide Area Access Points for  
Network Integrity and Coverage

2.2.2.1.2. Network Mesh Connectors to connect  
the topology where it can not be connected  
on the ground

#### 2.2.2.2. Example Equipment:

2.2.2.2.1. Static Aerial Node Payload such as  
the balloons utilized in COASTS 2006

2.2.2.2.2. Unmanned Air Ships that maintain a  
persistent presence

## 2.3. Gateways

### 2.3.1. Static Aerial Gateways

#### 2.3.1.1. Functions:

#### 2.3.1.2. Example Equipment

2.3.1.2.1. Payload onboard static aerial nodes (balloons) not unlike that utilized in COASTS 2006 at high altitudes for link integrity

2.3.1.2.1.1. UHF Link

2.3.1.2.1.2. VHF Link

2.3.1.2.1.3. 802.20 Link

2.3.1.2.1.4. 802.16 Link

2.3.1.2.1.5. Link-16 Link

2.3.1.2.1.6. SATCOM Link

## 2.4. Sensor Fusion Centers

### 2.4.1. Functions:

2.4.1.1. TDD

2.4.1.1.1. Prioritization

2.4.1.1.2. Queuing

2.4.1.1.3. Database of Targets

2.4.1.2. Common Picture Production

2.4.1.2.1. Map Layering

2.4.1.2.2. Target Layering

2.4.1.2.3. Sensor Feed Layering

2.4.1.2.4. TDD Layering

2.4.1.3. Real-Time Sensor Feeds

2.4.1.3.1. Prioritization

2.4.1.3.2. Layering of TDD on top of Video Streams

2.4.1.4. Example Equipment

2.4.1.4.1. Custom designed Hardware and Software Payload of Static Aerial Nodes that acts like a server to fuse together information and provide it to end-users

## 3. Rapid System Deployment Elements

### 3.1. Cluster Deployment of Ground Sensors

#### 3.1.1. Functions:

3.1.1.1. Modularity for deployment from a number platforms

3.1.1.2. Ability to create a redundant and robust deployment pattern for ground sensors

3.1.2. Example Equipment:

3.1.2.1. Deployed similar to the SFW

3.1.2.2. Deployed out of the back of a C-130 similar to humanitarian rations

3.2. Anchor Deployment of Gateways and Static Aerial Nodes

3.2.1. Functions:

3.2.1.1. Anchor the Static Aerial Nodes to the ground by a tether

3.2.2. Example Equipment

3.2.2.1. Modeled after the deployment of Sonobuoys coupled with the deployment of Jungle Penetrators (Anchors)

3.2.2.2. Pushed out of the back of a C-130 similar to that of humanitarian rations

3.3. Organic/Outside Deployment of Mobile Aerial Nodes/Sensors

3.3.1. Functions:

3.3.1.1. Flexible Sensors that can be controlled and focused on high priority targets and areas

3.3.1.2. Can serve as weapons action agents when armed

3.3.2. Example Equipment:

3.3.2.1. RQ-11A Raven UAV's

3.3.2.2. RQ-1 Predator

3.3.2.3. RQ-4A Global Hawk

4. End-User Interface Elements

4.1. Functions:

4.1.1. Provide common operational picture to the end-user consisting of a map and overlayed target data that can be viewed in layers

4.1.2. Provide access to prioritized sensor feeds to the end-user

4.1.3. Provide access to target data to the end-user

4.1.4. Provide a common operational picture of fused sensor data for SA

4.2. Example Equipment:

4.2.1. Modular PC's wearable PC's

4.2.2. Tacticomps

4.2.3. The HUD Helmet in development for the F-35 Joint Strike Fighter (JSF) which can overlay target data onto an individuals visual orientation of the scene

4.2.4. Blue Force Tracker (BFT)

**G. AERIALLY DEPLOYED SENSOR NET**

**1. Overview of the Model**

The system architecture for the sensor net will include a topology similar to that of the COASTS network or the Tactical Network Topology Program (TNT). It will be deployed aerially for rapid employment in the area of operation utilizing the sensor in depth doctrine for integration into Joint Operations.

The sensor in depth doctrine (Figure 34) will utilize multiple sensor layers from a strategic level providing global coverage (if necessary) to a tactical level. The strategic level will leverage national intelligence assets to localize the AO. Intelligence assets include imagery intelligence (IMINT), HUMINT, Signals Intelligence (SIGINT), and other global level assets that can identify a hot spot.

## Sensor-In-Depth

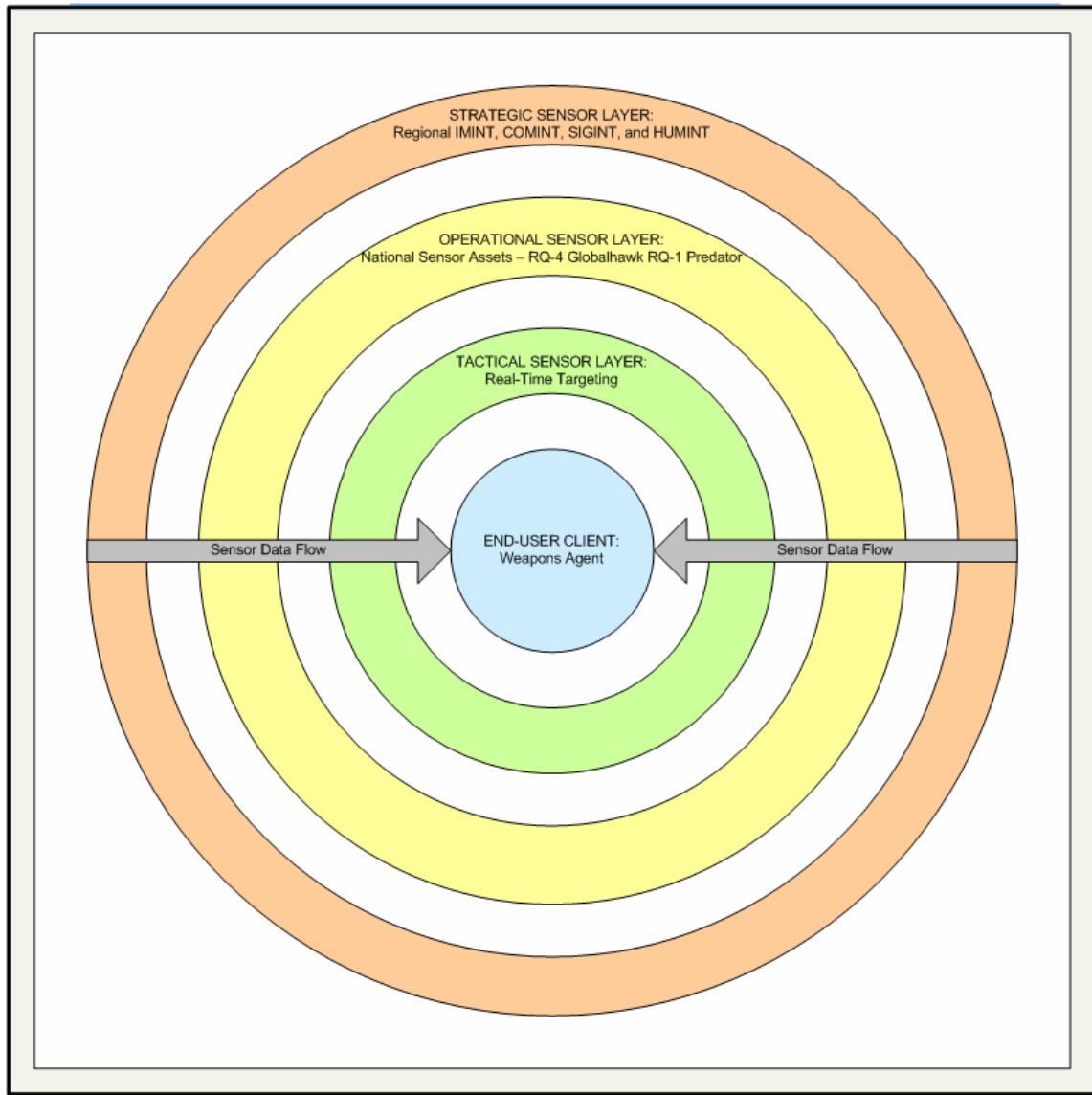


Figure 34. Sensor in Depth Layers

Necessary intelligence will be passed down to the next level, the operational sensor layer, for further localization within the AO. In addition, sensors will be deployed for passive patrolling of the AO to identify local operating areas containing possible targets of interest. Examples of patrolling elements at the operational level include RQ-1 Predator UAV's, RQ-4 Globalhawks (see Figure

35), and HUMINT. These localizers, once they identify an active target area, will pass the info downward for a closer look at the sensor net level.



Figure 35. RQ-4 Globalhawk ISR UAV Similar to the U-2 Spy Plane

The operational layer acts to localize threats further and trigger the deployment of the real-time sensor net establishing the tactical sensor layer. This will be a high tempo operation requiring real-time tactical targeting of targets within a pre-defined area passed down through the operational layer.

After deployment, backhaul gateways should be established and tested as should the full functionality of the system. Once fidelity and security is assured the

operation can discriminate, classify, and monitor targets in real-time. Standard doctrine will enable transmission of the targeting information to weapons action agents. Also, it is important to mention that the sensor net should be highly redundant to ensure fidelity of the information and establish appropriate feeds.

#### **H. IMPLEMENTATION OF SENSOR NET**

COTS technology can be a big cost advantage to the real-time sensor net. Following is an itemized list of the technologies that could be utilized:

- Cyber Defense Systems CyberBUG mini-UAV Drone
  - Lightweight surveillance, reconnaissance, target acquisition
- Rotomotion SR20 Vertical Takeoff and Landing (VTOL) UAV Helicopter System
  - Surveillance, reconnaissance, target acquisition, network extension, sensor deployment
- Crossbow Wireless Ad-hoc Sensor Network
  - Infrared and magnetic anomaly sensors for security and tracking
- CACI/Cisco Tactical Communications Kit (TCK)
  - Ruggedized rapidly-deployable, secure voice, data, and video communications open-standard Internet Protocol router, interfaces Cisco Voice over Internet Protocol (VoIP), wireless, satellite, and land mobile radio (LMR) connectivity (LMRoIP)
- Harris AN/PRC-117 ground-to-air havequick I/II radio system
  - HF/VHF/UHF (30-512 MHz) reprogrammable digital radio
- Harris AN/PRC-150 man pack radio system

- NSA certified HF/VHF radio for secure voice and data (9600 bps) communication up to 60 MHz
- SecNet 11 National Security Agency (NSA) Certified 802.11 Encryption
- XACTA Deployable Wireless Mesh Nodes
- Tachyon tactical SATCOM equipment
- Integrated Blimp Works' 10'/13' Ball Balloons and My-te Winch Hoists
  - Equipped with MeshDynamics Network Devices and Antennas to act as network extenders at 4,500 feet
- IEEE 802.11, 802.16, and 802.20 wireless protocols
- MeshDynamic Systems (MDS) 802.16/11 Boxes
- A Mobile Network Operations Center (MNOC) titled "Nemesis"
- Two way radio integration of Land Mobile Radio over IP (LMRoIP), ARC over IP (ARCoIP), SATCOMoIP, and Voice over (VoIP) for backhaul gateways
- MDS DenyGPS

The suggested sensor net could easily be jammed by a national level force's technology (i.e. China or Iran). However, this system is designed for decomposed forces that will most likely not have the capability to jam or even detect such a system as having been set up.

THIS PAGE INTENTIONALLY LEFT BLANK

## **V. SYSTEM SOLUTION AND FUTURE DEVELOPMENT**

The purpose of this investigative study was to suggest a model for a system of systems which improves real-time targeting through an aerially deployed wireless mesh sensor network.

### **A. FUTURE DEVELOPMENTS**

#### **1. Path to a Solution**

The path to a solution is multifaceted and multi-tasked. Paths to a proven concept should thus include the following components:

- Experimentation for Development of MOP's
- Additional Survey for Development of MOP's
- LLNL Guardian Sensors
- In depth research by established foundation SPAWAR
- Survey, ruggedized, and reliable COTS equipment

Prioritization algorithms need to be developed, given the input of TDD and coordinates and high value asset coordinates. These algorithms should be modular and flexible to the requirements of the AO (geographical, political, current forces in the area, threat intelligence, threat priorities (i.e. if they're carrying drugs, rifles, or IEDs)).

The path to a solution also requires network development and gateway integration. Transmission medium must be developed to be robust, secure, and self healing. Gateway interoperability must be developed for the aerial payloads. Interoperability with SATCOM, UHF, Link-16, and even 802.20 must be utilized.

Common operational picture interface also need be developed for a heavily layered simplistic interface. The interface should take full use of input commands from human operators including acoustic, conventional tactile, and even motion patterning input methods. Output will require refinement to create a seamless information flow to the operator in the least restrictive manner possible utilizing a head mounted HUD or wearable PC.



Figure 36. Ruggedized MTM Micro Tablet by Modular PC  
(From: <http://modular-pc.com/>, Retrieved March 2, 2006)

In addition, the path to a solution requires a number of other tasks and activities. These have been summarized and presented in list form as follows:

- LLNL Guardian Sensors for the foundation of the sensor net to produce layers.

- Integration of UAV's - RQ-11 Raven, RQ-1 Predator, RQ-4 Global Hawk links into static aerial sensor fusion center.
- Sensor fusion payloads which accept multiple inputs from different layers.
- A static aerial node deployment method, not unlike the canopy penetrators utilized in Vietnam, but with balloons that inflate quickly.
- Integration of already existing IR and near IR sensors.
- Static ground sensors deployed as a cluster munitions like the SFW.
- Man-portable mobile ground real-time sensor feeds for flexible first person operator views.
- Modular systems for urban ops, jungle ops, mountain ops, and desert ops; all built from common modules.
- UWB analyses for ability penetration of opaque environments.
- Long life power supplies of all equipment (gridpoint renewable power sources).
- Airborne Sensor Fusion Centers for TDD layering technology. For example, the London subways use of UWB sensors to layer target data onto a real-time visual feed literally drawing a box around a weapon a person is carrying.
- Integrate GPS systems into all sensor nodes for positional layering purposes and FOV calculation in addition to outputting accurate grid coordinates to weapons.
- Efficient GUI interface for the common operational picture. The interface should be developed in a layered system displaying top level data that can be drilled downwards and access feeds.

The path to a solution also involves doctrine development. It is important to categorize hostile stance imagery from real-time sensor feeds and integration into training doctrine for TDD rules of engagement (ROE). That

is, what TDD weapon kill and answer the question as to how much sensor data is required to initiate weapon action on a target. There is also a need to experiment with optimal aerial deployment pattern for the Sensor Net (not unlike the deployment patterns for sonobuoy sub hunting)

Interface doctrine must also be created. It should be determined as to who is allowed to control the focus of limited real-time sensor feed assets and how many sensor interface units are required by local area operators within the net. In addition, it is important to develop doctrine for utilization of real-time sensor feeds and determine when to monitor them, what information is required, and how reliable are they.

#### **B. FUTURE RESEARCH**

Future research should focus on a survey of. Such a survey should include SOF, Airborne Attack Craft, Attack UAV's, and target prosecuting forces.

Future research should also focus on test beds and delivering products to the end user. It is important to work closer with end-users to identify essential products and simplify needs.

In addition, future research should experiment with the ability/use of ground sensor feeds. Such research should try to answer the questions, "Are they feasible?" "Does a pattern of randomly spread real-time sensor feeds assist in SA?"

It is also important to research the interoperability links of the RQ-4A Global Hawk, the RQ-11A Raven, and the RQ-1 Predator. What links will be required on the Gateway

Payload to link to these organic and outside assets? This was an issue when linking the Cyberbug UAV and the Rotomotion UAV into the COASTS 2006 network. Since links were in different formats, the UAVs lacked interoperability.

The following specific research studies need to be performed:

1. A research study on the prioritization/queuing of TDD should be performed. How should targets/local operating areas be optimally prioritized by algorithms? How will this vary in varying AO's, urban vs. triple canopy jungle, political insurgencies vs. genocide?
2. Research the network layers. To determine what it can support, how it can integrate with sensor feeds and when overload occurs.
3. Examine feasibility of uplinking data to an aerial attack craft and seeing how much SA could be provided.
4. Investigate the feasibility of a common operational picture being inserted into an aircraft. Such a study should ask, how can this be accomplished? Will that be useful? How much targeting can be achieved with it? Can airborne attack assets control their own weapons release and identify targets with the interface link from the common operational picture? To whom other than on scene operators will the common operational picture be disseminated?
5. Research security protocol during real time operations for an UWB physical layer (Secnet.11 NSA certified security encryption for 802.11 already exists, so it is feasible to apply to UWB communications). In addition, natural security features of UWB frequency hopping should be investigated.
6. Research altitude requirements for the transmission medium payload of the static aerial nodes (balloons). Finally, the pattern of graduated heights should be investigated to

determine a lower layer of sensor net coverage and an upper layer of sensor fusion centers with gateway backhauls.

7. Research gateway nodes to determine how they should be linked - what SATCOM links, with forward operating bases, with intelligence centers? What kind of doctrine should be developed for the gateway nodes? To whom should they report?
8. How should data be classified coming from the Sensor Net if it can be made available to a wider military community via the gateways. What doctrine could be developed for the control of the data dissemination?
9. Future research should determine whether local area operators utilizing the transmission medium and the targeting net can to release weaponry onto targets.

The solution exists in the potential technological-doctrinal capabilities of our society to overcome current targeting discrepancies and meet the asymmetric threat of ideological hatred faced in opaque environments globally through an aerially deployed, real-time targeting, sensor net.

## **APPENDIX A. ACRONYMS**

AO	Area of Operations
AOR	Area of Responsibility
ATO	Air Tasking Order
BFT	Blue Force Tracker
C2	Command and Control
CA	Civil Affairs
CBT	Combating Terrorism
COASTS	Coalition Operating Assisted Surveillance and Targeting System
COCOM	Combatant Commander
COIN	Counter Insurgency
COP	Common Operational Picture
COTS	Commercial off The Shelf
DA	Direct Action
DoD	Department of Defense
DSS	Distributed Spread Spectrum
FID	Foreign Internal Defense
FLAK	Fly Away Kit
GPS	Global Positioning System
GWOT	Global War on Terrorism
GUI	Graphical User Interface
HAHO	High Altitude High Opening
HALO	High Altitude Low Opening
HF	High Frequency
HN	Host Nation
HUD	Heads up Display
HUMINT	Human Intelligence
IED	Improvised Explosive Device
IO	Information Operations
IP	Internet Protocol
IR	Infrared
ISR	Intelligence, Surveillance, and Reconnaissance

JC4ISR	Joint Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance
JIATF-W	Joint Interagency Task Force West
JSOTF	Joint Special Operations Task Force
LAN	Local Area Network
LLNL	Lawrence Livermore National Laboratory
LPI	Low Probability of Intercept
MGRS	Military Grid Reference System
MNOC	Mobile Network Operations Center
MOE	Measures of Effectiveness
MOOTW	Military Operations Other Than War
MOP	Measures of Performance
NASA	National Aeronautics and Space Association
NOAA	National Oceanic and Atmospheric Administration
NPS	Naval Postgraduate School
NPSSOCFEP	Naval Postgraduate School Special Operations Field Experimentation Program
OE	Opaque Environment
OEF	Operation Enduring Freedom
OFDM	Orthogonal Frequency Division Multiplexing
OIF	Operation Iraqi Freedom
PRF	Pulse Repetition Frequency
PSYOP	Psychological Operations
RMSI	Regional Maritime Security Initiative
ROE	Rules of Engagement
RTA	Royal Thai Army
RTAF	Royal Thai Air Force
SATCOM	Satellite Communications
SFW	Sensor Fuzed Weapon
SOF	Special Operations Force
SOSUS	Sound Surveillance System
TDG	Technological-Doctrinal Gap
TNT	Tactical Network Topology
TOC	Tactical Operations Center
TR	Tactical Reconnaissance

UAV	Unmanned Aerial Vehicle
UHF	Ultra High Frequency
USPACOM	United States Pacific Command
USSOCOM	United States Special Operations Command
UWB	Ultra Wideband
VBSS	Visit Board Search and Seizure
VTOL	Vertical Takeoff and Landing
VHF	Very High Frequency
WLAN	Wireless Local Area Network
WMD	Weapons of Mass Destruction

THIS PAGE INTENTIONALLY LEFT BLANK

## **APPENDIX B. MEASURES OF EFFECTIVENESS**

1. Deliver target discrimination data between targets and non-combatants utilizing hostile equipment on the target and coordinates of the target(s)
2. Deliver Highly Accurate Grid Coordinates layered with target discrimination data. Data should be filtered out for modularity purposes.
3. Provide a real-time visual (visual, IR, near IR, or UWB produced) sensor feed on the target layered with target discrimination data, FOV data.
4. Prioritize multiple real-time sensor feeds by target discrimination data and number of targets autonomously.
5. Multiple targets must be queued up in order of priority based upon target data autonomously.
6. Generate a layered common operational picture of all targets by fusing all sensor data together.
7. From the common operational picture allow portal type access to layered real-time sensor feeds, and layered individual target data.
8. Disseminate the common operational picture beyond the tactical force for Joint Operations empowerment and force situational awareness.
9. Sensor operations and data filtering should be in complete control of the on scene operator(s).
10. The system must be rapidly deployable within the time frame of a half an hour.
11. Operators must have direct interface with data from the sensor net in visual and auditory interfaces.

12. The system must be modular, allowing for a variety of preplanned and ad-hoc environmental variances.
13. Above all the system goal must be to bootstrap and empower the on scene commander to accomplish the mission.

**APPENDIX C. COALITION OPERATING AREA SURVEILLANCE  
AND TARGETING SYSTEM (COASTS) THAILAND FIELD  
EXPERIMENT (MAY 2006)**

In FY2006 the Naval Postgraduate School (NPS) carried out a research program entitled the Coalition Operating Area Surveillance and Targeting System (COASTS). The COASTS field experimentation program supports U.S. Pacific Command (USPACOM), Joint Interagency Task Force West (JIATF-W), Joint U.S. Military Advisory Group Thailand (JUSMAGTHAI), U.S. Special Operations Command (USSOCOM), NPS, Royal Thai Armed Forces (RTARF), and the Thai Department of Research & Development Office (DRDO) science and technology research requirements relating to theater and national security, counter-drug and law enforcement missions, and the War On Terror (WOT). This CONOPS is primarily intended for use by the NPS and RTARF management teams as well as by participating commercial partners. However, it may be provided to other U.S. Government (USG) organizations as applicable. This document describes research and development aspects of the COASTS program and establishes a proposed timetable for a cap-stone demonstration during May 2006 in Thailand.

**A. BACKGROUND**

The COASTS programmatic concept is modeled after a very successful ongoing NPS-driven field experimentation program entitled the NPS-U.S. Special Operations Command Field Experimentation Program (NPSSOCFEP). NPSSOCFEP is executed by NPS, in cooperation with USSOCOM and several contractors, and has been active since FY2002. Program inception supported USSOCOM requirements for integrating

emerging wireless local area network (WLAN) technologies with surveillance and targeting hardware/software systems to augment Special Operations Forces (SOF) missions. NPSSOCFEP has grown significantly since inauguration to include 10-12 private sector companies who continue to demonstrate their hardware/software capabilities, several DoD organizations (led by NPS) who provide operational and tactical surveillance and targeting requirements, as well as other academic institutions and universities who contribute a variety of resources.

NPSSOCFEP conducts quarterly 1-2 week long complex experiments comprising 8-10 NPS faculty members, 20-30 NPS students, and representatives from multiple private companies, DoD and US government agencies. Major objectives are as follows:

- Provide an opportunity for NPS students and faculty to experiment/evaluate with the latest technologies which have potential near-term application to the warfighter.
- Leverage operational experience of NPS students and faculty
- Provide military, national laboratories, contractors, and civilian universities an opportunity to test and evaluate new technologies in operational environments
- Utilize small, focused field experiments with well-defined measures of performance for both the technologies and the operator using the technologies
- Implement self-forming / self-healing, multi-path, ad-hoc network w/sensor cell, ground, air, and satellite communications (SATCOM) network components

## LIST OF REFERENCES

- Abdelzaher, T.F., et al. (2003). *EnviroTrack: Environmental programming model for tracking applications in distributed sensor networks*. (Tech. Rep. No. CS-2003-02). Charlottesville, Virginia: University of Virginia.
- Aboelaze, M., and Aloul, F. (2005). Current and future trends in sensor networks: a survey. *Wireless and Optical Communications Networks, 2005. WOCN 2005. Second IFIP International Conference*, March 6-8, 2005.
- Adamy, D. (2004). *EW 101: A first course in electronic warfare*. Norwood, Massachusetts: Artech House Publishers.
- Akyildiz, I.F., Weilian, S., Sankarasubramaniam, Y., & Cayirci, E. (2002, August). A survey on sensor networks. *Communications Magazine, IEEE*, 40(8), 102-114.
- Aloul, F., and Aboelaze, M. (2005, March). Current and future trends in sensor networks: A survey. *Wireless and optical communications networks, 2005. Second IFIP International Conference*, March 6-8, 2005.
- Bach, E.J., and Fickel, M.G. (2004, September). *An analysis of the feasibility and applicability of IEEE 802.X wireless mesh networks within the global information grid*. Unpublished master's thesis. Naval Postgraduate School, Monterey, California.
- Bowie, C., Haffa, R. and Mullins, R. (2003). *Future war: What trends in America's post-cold war military conflicts tell us about early 21<sup>st</sup> century warfare*. Washington D.C., Northrop Grumman Analysis Center.
- Braden, N. (2006, May). Reading the signs of threat transformation. *Proceedings*, 61.
- Bragnisky, D., and Estrin, D. (2002, September). Rumor routing algorithms for sensor networks. *Proceedings of Association for Computer Machinery Workshop on Wireless Sensor Networks and Applications*, 22-31.
- Callaway, Jr., E. (2004). *Wireless sensor networks architectures and protocols*. New York: Auerbach Pub.

Central Intelligence Agency (2005). *Thailand: World Factbook 2005*. Office of Public Affairs. Retrieved June 2, 2006 from  
<http://www.cia.gov/cia/publications/factbook/geos/th.html>

Chong, C., and Kumar, S. (2003, August). Sensor networks: Evolution, opportunities, and challenges. *Proceedings of the IEEE*, 91(8), 1247-1256.

Clark, V. (2002, October). Sea Power 21. *Proceedings*, Retrieved April 3, 2006, from  
<http://www.chinfo.navy.mil/navpalib/cno/proceedings.html>.

Coalition Operating Area Surveillance and Targeting System (COASTS) (2006, May). *Thailand field experiment: Concept of operations*. Naval Postgraduate School. Monterey, California.

Cooklev, T. (2004). *Wireless communication standards: A study of IEEE 802.11, 802.15 and 802.16*. New York: IEEE Press.

Cravotta, N. (2002, October 17). *Ultrawideband: The next wireless panacea?* Retrieved June 3, 2006 from  
<http://www.edn.com/article/ca250832.html>.

Creswell, J. W. (2003). *Research design, qualitative, quantitative, and mixed methods approaches*. Second edition. Thousand Oaks, California: Sage.

Crossbow. (2003). Retrieved June 2, 2006 from  
<http://www.xbow.com/Products/Product-pdf-files/MICAO/o20data%20sheet.pdf>.

DeBardelaben, J.A. (2003, November). Multimedia sensor networks for ISR applications. *Signals, Systems and Computers. Conference Record of the Thirty-Seventh Asilomar Conference*, 2, 2009-2012.

Fenton, S. J. (1999). *Global broadcast service reach back via satellite tactical digital link J (S-tadil J)*. Unpublished Master's Thesis. Naval Postgraduate School, Monterey, California.

Fraden, J. (2004). *Handbook of modern sensors* (2<sup>nd</sup> ed.). New York: Springer-Verlag.

- Halvardsson, M., and Lindberg, P. (2004, February 14). *Reliable Group Communication in a Military Mobile Ad hoc Network*. Unpublished master's thesis, Vaxjo, Sweden: Vaxjo University.
- He, T., Stankovic, J.A., Lu, C., and Abdelzaher, T. (2003, May). SPEED: A stateless protocol for real-time communications in sensor networks. *Proceedings of IEEE International Conference on Distributed Computing Systems 2003*, 46-57d.
- Herzig, J. F. Jr. (2005, March). *An analysis of the feasibility of implementing ultra wideband and mesh network technology in support of military operations*. Master's Thesis. Naval Postgraduate School, Monterey, California.
- Hill, J., Szewczyk, R., Woo, A., Hollar, S., Culler, D., and Pister, K. (2000, Nov.). System architecture directions for networked sensors. *Proceedings of Architectural Support for Programming Languages and Operating Systems*, Boston, Massachusetts, 93-104.
- Hu, Z., & Li, B. (2004). On the fundamental capacity and lifetime limits of energy-constrained wireless sensor networks. *Real-Time and Embedded Technology and Applications Symposium, 2004. Proceedings. Real-Time and Embedded Technology and Applications Symposium 2004. 10th IEEE*, 2-9.
- Innovative Wireless Technologies. (2006). Sensors networks, wireless sensor network development. Retrieved June 1, 2006 from <http://www.iwtwireless.com/SensorNetworks.htm>.
- Intel. (2005, February). *Ultra-wideband (UWB) technology. Enabling high-speed wireless personal area networks*. Retrieved March 10, 2006 from <http://www.intel.com/technology/comms/uwb/download/ultra-wideband.pdf>.
- Joint Vision 2020. (2000, June). US Government Printing Office. Retrieved May 10, 2006 from <http://www.dtic.mil/jointvision/jvpub2.htm>.
- Karlof, C., and Wagner, D. (2003, May). Secure routing in wireless sensor networks: Attacks and countermeasures. *Proceedings of IEEE Workshop on Sensor Networks Protocols and Applications*.

- Lim, A. (2001, September). Distributed services for information dissemination in self-organizing sensor networks. *Journal of Franklin Institute*, 338(6), 707-727.
- Lu, C., Blum, B., Abdelzaher, T., Stankovic, J., and He, T. (2002, September). RAP: Real-time communication in sensor networks. *Proceedings of IEEE Real Time and Embedded Technology and Applications Symposium 2002*, 55-66.
- MESHDynamics. (2005). Why structured MESH is different. Retrieved May 1, 2006 from <http://www.MESHdynamics.com/WhyStructuredMESH.html>.
- Navy Concept Development and Experimentation Expeditionary Power Projection. (2001, June). Retrieved February 2, 2006 from <http://www.dtic.mil/ndia/2001ewc/ncde.pdf>.
- Nekoogar, F. (2005). *Ultra-Wideband Communications-Fundamentals & Applications*. Upper Saddle River, NJ: Prentice Hall.
- Pahlavan, K., and Krishnamurthy, P. (2004). *Principles of wireless sensor networks*. Upper Saddle River, NJ: Prentice Hall.
- Parr, S. (2003, July). New threats to human security in the era of globalization. *Journal of Human Development*, 4(2), 167-179.
- Pierson, J. (2001, May). Entran tech tips-miniature sensors: When, where and why should we use them? Pierson & Associates. Retrieved January 28, 2006 from <http://www.entranc.com/TechTipPart1.htm>.
- Rabaey, J., Ammer, M., da Silva, J., Patel, D., & Roundy, S. (2000, July). PicoRadio supports adHoc ultra-low power wireless networking. *IEEE Computer*, 33(7), 42-48.
- Ricks, T. E. (2006, February 21)). U.S. counterinsurgency academy giving officers a new mind-set. *Washington Post*, A10.
- Roberts, M., Trace, M., and Klein, A. (2004). *Thailand's war on drugs. The Beckley Foundation Drug Policy Programme*. A Drugscope Briefing Paper.

- Shreves, K. W. (2004, April). *National military strategy and the GWOT – Choosing the means*. Maxwell Air Force. Course 5605. Retrieved June 2, 2006 at  
[http://www.maxwell.af.mil/au/awc/awcgate/ndu/shreves\\_gwot\\_strat.pdf](http://www.maxwell.af.mil/au/awc/awcgate/ndu/shreves_gwot_strat.pdf).
- Subramanian, L., and Katz, R.H. (2000). An architecture for building self-configurable systems. *Mobile and Ad Hoc Networking and Computing, 2000. MobiHOC*, 63-73.
- Suh, J., and Horton, M. (2005). Current hardware and software technology for sensor networks. Retrieved March 2, 2006 from  
[http://www.unl.im.dendai.ac.jp/INSS2004/INSS2004\\_papers/ShortPresentations/H7.pdf](http://www.unl.im.dendai.ac.jp/INSS2004/INSS2004_papers/ShortPresentations/H7.pdf).
- Tseng, V.S., and Lin, K.W. (2005). Mining temporal moving patterns in object tracking sensor networks. *Ubiquitous Data Management, 2005. International Workshop*, 105-112.
- Turon, M., Horton, M., Hill, J., and Broad, A. (2005, February). XMesh Routing Layer. *TinyOS Technology Exchange*. Retrieved March 3, 2006  
<http://www.tinyos.net/ttx-02-2005/>.
- Van Dyck, R.E., and Miller, L.E. (2001, October). Distributed sensor processing, over an ad hoc wireless network: Simulation framework and performance criteria. Retrieved March 2, 2006  
<http://w3.antd.nist.gov/pubs/milcom01.pdf>.
- Vent, D. *BioNet Program Overview*. County of San Diego Department of Environmental Health. Retrieved March 2, 2006 from  
<http://www.nlectc.org/training/nij2005/Vent.pdf>.
- Werner-Allen, G., Swieskowski, P., & Welsh, M. (2005). MoteLab: A wireless sensor network testbed. *Information Processing in Sensor Networks, 2005. IPSN 2005. Fourth International Symposium*, 483-488.
- Wilson, J. M. (2002, September 10). *Ultra-wideband/a disruptive RF technology?* Retrieved June 4, 2006 from  
<http://www.intel.com/technology/comms/uwb/download/Ultra-Wideband%20Technology.pdf>.

Ye, F., Chen, A., Lu, S., & Zhang, L. (2001, October). A scalable solution to minimum cost forwarding in large sensor networks. *Proceedings of IEEE International Conference on Computers Communications and Networks 2001*, 304-309.

## **INITIAL DISTRIBUTION LIST**

1. Defense Technical Information Center  
Ft. Belvoir, Virginia
2. Dudley Knox Library  
Naval Postgraduate School  
Monterey, California
3. Dr. Orin E. Marvel  
Naval Postgraduate School  
Monterey, California
4. LtCol Karl D. Pfeiffer, Ph.D.  
Naval Postgraduate School  
Monterey, California
5. Mr. James Ehlert  
Naval Postgraduate School  
Monterey, California
6. Commanding Officer  
SPAWARSCEN  
San Diego, California
7. Dr. Marion Ceruti  
SPAWARSCEN  
San Diego, California
8. Ms. Rita Painter  
Naval Postgraduate School  
Monterey, California
9. Dr. Gurmindar Singh  
Naval Postgraduate School  
Monterey, California
10. Col Brian Greenshields  
Naval Postgraduate School  
Monterey, California
11. LTC Gregory Wilson  
Naval Postgraduate School  
Monterey, California

12. MAJ Ewing  
Naval Postgraduate School  
Monterey, California
13. Professor Bill Kemple  
Naval Postgraduate School  
Monterey, California
14. Mr. Ivan Cardenas  
Kestrel Technology Group  
Houston, Texas
15. CAPT Phil Erdie  
US Marine Corps Systems Command (MARCORSYSCOM)  
Quantico, Virginia
16. Col Thomas Lee Williams  
U.S. Pacific Command  
Camp Smith, Hawaii
17. Mr. Jim Alman  
CyberDefense UAV Systems  
Saint Petersburg, Florida
18. Mr. Dennis B. D'Annunzio  
COO, Rotomotion, LLC  
459 Jessen Lane, Suite C  
Charleston, South Carolina
19. Group Captain Teerachat Krajomkeaw  
Directorate of Operations  
Royal Thailand Air Force (RTAF) Headquarters  
Bangkok, Thailand
20. NETWARCOM, FORCENet Execution Center - West  
BLDG 16  
San Diego, California
21. CDR Phil Rigier  
Joint Special Operations Task Force - Philippines  
Camp Navarro, Philippines
22. CDR Fred Kacher  
Chief of Naval Operations (OPNAV)  
Information, Plans and Strategy (N3/N5)  
Washington, District of Columbia

23. LCDR Christopher Sweeney  
Chief of Naval Operations (OPNAV)  
Information, Plans and Strategy (N3/N5)  
Washington, District of Columbia
24. Mr. Peter A. Landauer  
Gridpoint, Inc.  
Baltimore, Maryland
25. Mr. Thomas Latta  
C4ISR & IO PM  
Space and Naval Warfare Systems Command  
DOT&E IA&I/IO OT&E Branch, COMOPTEVFOR  
San Diego, California
26. Dr. Dan Boger  
Naval Postgraduate School  
Monterey, California